6712-01

This document is scheduled to be published in the Federal Register on 11/17/2020 and available online at **federalregister.gov/d/2020-24904**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket No. 17-97; FCC 20-136; FRS 17172]

Call Authentication Trust Anchor

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) adopts rules implementing the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), promoting the deployment of caller ID authentication technology, and combatting the practice of illegal caller ID spoofing. In doing so, the Second Report and Order adopts rules governing intermediate providers and caller ID authentication in non-IP networks, implementing the exceptions and extensions established by the TRACED Act, and prohibiting line-item charges for caller ID authentication.

DATES: Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, except for instruction 10 (§ 64.6306) which is effective [**INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and instruction 6 (§ 64.6303(b)), instruction 9 (§ 64.6305(b) and (c)), and instruction 11 (§ 64.6306(e)) which are delayed indefinitely. The Commission will publish a document in the **Federal Register** announcing the effective date of these instructions.

FOR FURTHER INFORMATION CONTACT: For further information, please contact Mason Shefa, Competition Policy Division, Wireline Competition Bureau, at Mason.Shefa@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Second Report and Order* in WC Docket Nos. 17-97, FCC 20-136, adopted on September 29, 2020, and released on October 1, 2020. The full text of this document is available for public inspection on

the Commission's website at: https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf.

The Commission received approval from the Office of Management and Budget (OMB) on November 2, 2020, for a period of six months, of the information collection requirements relating to the voluntary implementation exemption certification rules contained in § 64.6306, which shall be effective upon publication in the **Federal Register** pursuant to 5 U.S.C. 553(d)(1). The OMB Control Number is 3060-1278. The Commission publishes this document as an announcement of the effective date of the rules. The total number of respondents and total annual responses are 817, the total annual burden hours are 2,451 and no costs are associated with this information collection. At a later time, the Commission will seek OMB approval of §§ 64.6303(b), 64.6305(b), and 64.6306(e) and the information collection requirements contained therein.

I. INTRODUCTION

1. Protecting Americans from the dangers of unwanted and illegal robocalls is our top consumer protection priority. More than just an annoyance, these calls are a tool for scammers to take advantage of unsuspecting Americans. Bad actors often "spoof" or falsify caller ID information and deceive call recipients into believing they are trustworthy. Even in the midst of the COVID-19 pandemic, bad actors have continued their attempts to use illegal spoofing to target American consumers, once again illustrating the pervasiveness of this problem.

2. As part of our multi-pronged approach to combat this vexing issue, we have made it a priority to stop the practice of illegal caller ID spoofing. For instance, we have issued hundreds of millions of dollars in fines for violations of our Truth in Caller ID rules. We recently proposed a forfeiture of $225 million—the largest in the Commission's history—for a company that made approximately one billion spoofed robocalls, and we proposed two forfeiture actions of almost $13 million and $10 million apiece against other entities for apparent spoofing violations. We have expanded our Truth in Caller ID rules to reach foreign calls and text

messages. Pursuant to the TRACED Act, we have selected a consortium to conduct private-led traceback efforts of suspected illegal robocalls, which is particularly useful in instances where the caller ID information transmitted with a call has been maliciously spoofed. We have clarified and bolstered our call blocking rules to give voice service providers new latitude to block calls, including spoofed calls.

3. One key part of our broad efforts to thwart illegal caller ID spoofing has been our work to promote implementation of the STIR/SHAKEN caller ID authentication framework. The STIR/SHAKEN framework allows voice service providers to verify that the caller ID information transmitted with a particular call matches the caller's number, while protecting consumer privacy and promoting the ability to complete lawful calls. Widespread implementation of STIR/SHAKEN will reduce the effectiveness of illegal spoofing, allow law enforcement to identify bad actors more easily, and help voice service providers identify calls with illegally spoofed caller ID information before those calls reach their subscribers. We have worked over the course of multiple years to promote caller ID authentication, and in 2019 Congress amplified our efforts by passing the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, which directs the Commission to take numerous steps to promote and require STIR/SHAKEN implementation. In March of this year, building on the foundation laid by our prior work and by Congress, we adopted rules requiring voice service providers to implement the STIR/SHAKEN call authentication technology in the internet protocol (IP) portions of their phone networks by June 30, 2021 (85 FR 22029, April 21, 2020).

4. In this document, we continue our work to promote the deployment of caller ID authentication technology and to implement the TRACED Act. After consideration of the record, we adopt rules implementing many of the proposals we made in the *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking (FNPRM)* (85 FR 22029, April 21, 2020 and 85 FR 22099, April 21, 2020). Among other things, we adopt rules

governing intermediate providers and caller ID authentication in non-IP networks, we implement the exceptions and extensions established by the TRACED Act, and we prohibit line-item charges for caller ID authentication.

II. BACKGROUND

5. As the telecommunications industry has advanced and expanded into IP-based telephony, costs have decreased as competition increased, benefitting consumers greatly. These benefits, however, have eroded the chains of trust that previously bound voice service providers together. Partly due to the rise of the Voice over Internet Protocol (VoIP) software, the telephony industry no longer consists only of a limited number of carriers that all trusted each other to provide accurate caller ID information. Because there are now a multitude of voice service providers and entities originating and transiting calls, bad actors can more easily take advantage of these weakened chains of trust to target consumers with illegally spoofed calls.

6. Recognizing this vulnerability, technologists from the Internet Engineering Task Force (IETF) and the Alliance for Telecommunications Industry Solutions (ATIS) developed standards to allow the authentication and verification of caller ID information for calls carried over IP networks using the Session Initiation Protocol (SIP). Since voice service providers could no longer count on the multitude of entities in each call path to accurately pass the caller ID information, the goal was to create a system that allowed the identification information to safely and securely travel with the call itself. The result is the STIR/SHAKEN call authentication framework.

7. The framework is comprised of several different standards and protocols. The Secure Telephony Identity Revisited (STIR) working group, formed by the IETF, has produced several protocols for authenticating caller ID information. ATIS, together with the SIP Forum, produced the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification, which standardizes how the protocols produced by STIR are implemented across the industry using digital "certificates." At a high-level, the STIR/SHAKEN framework consists

of two components: (1) the technical process of authenticating and verifying caller ID information; and (2) the certificate governance process that maintains trust in the caller ID authentication information transmitted along with a call.

8. *Technology*. The STIR/SHAKEN technical authentication and verification processes rely on public key cryptography to securely transmit the information that the originating voice service provider knows about the identity of the caller and its relationship to the phone number it is using throughout the entire length of the call path, allowing the terminating voice service provider to verify the information on the other end. In this Report and Order, we use the term "caller" to broadly refer to the person or entity originating a voice call. We recognize that for the purpose of industry standards or other technical documents, this relationship may be described using more exact language suited to the specific technical scenarios described. The encrypted caller ID information is contained within a unique header to the message used to initiate a SIP call (the SIP INVITE message), called an "Identity" header. While there is no technical mechanism within the STIR/SHAKEN framework that ensures this Identity header travels the entire length of the call path unaltered, the unbroken transmission of an unaltered Identity header from the originating voice service provider, through each intermediate provider, to the terminating voice service provider is critical to creating the end-to-end chain of trust that allows a terminating provider to know it has received accurate caller ID information.

9. Because providers transmit the Identity header in a SIP INVITE and because SIP is IP-based, STIR/SHAKEN only operates in the IP portions of a provider's network. If a call originates on a non-IP network, that voice service provider cannot authenticate the caller ID information; if it terminates on a non-IP network, that voice service provider cannot verify the caller ID authentication information. And if a call is routed at any point over an interconnection point or intermediate provider network that does not support the transmission of SIP calls, the Identity header will be lost. While standards bodies are currently working on non-IP call authentication solutions, and some vendors are developing potential non-IP solutions, there is yet

to be an industry consensus on the path forward.

10. In the STIR/SHAKEN framework, the provider adding the Identity header to the SIP INVITE can use three different levels of attestation to signify what it knows about the identity of the calling party. The highest level of attestation is called full or A-level attestation. A provider assigns an A-level attestation when it is the entry point of the call onto the IP network, it can confirm the identity of the subscriber making the call, and the subscriber is using its associated telephone number. The method or process a provider uses to determine the legitimacy of the caller's use of a telephone number is specific to each provider. As a result, a provider's reputation is tied to the rigor of its evaluation process. The middle level of attestation is called partial or B-level attestation. A provider uses a B-level attestation to indicate that it is the entry point of the call onto the IP network and can confirm the identity of the subscriber but not the telephone number. The lowest level of attestation is called gateway or C-level attestation. A provider uses a C-level attestation when it is the point of entry to the IP network for a call that originated elsewhere but has no relationship with the initiator of a call, such as when a provider is acting as an international gateway. A downstream provider can make use of a C-level attestation to trace a call back to an interconnecting service provider or the call's entry point into the IP network. The STIR/SHAKEN standards envision these various attestation levels as information that can facilitate traceback and to enhance the spam identification solutions that terminating voice service providers enable for their customers.

11. *Governance*. The STIR/SHAKEN framework relies on digital "certificates" to ensure trust. The voice service provider adding the Identity header includes its assigned certificate which says, in essence, that the voice service provider is the entity it claims to be and that it has the right to authenticate the caller ID information. To maintain trust and accountability in the voice service providers that vouch for the caller ID information, a neutral governance system issues the certificates. The STIR/SHAKEN governance model requires several roles in order to operate: (1) a Governance Authority, which defines the policies and

procedures for which entities can issue or acquire certificates; (2) a Policy Administrator, which applies the rules set by the Governance Authority, confirms that certification authorities are authorized to issue certificates, and confirms that voice service providers are authorized to request and receive certificates; (3) Certification Authorities, which issue the certificates used to authenticate and verify calls; and (4) the voice service providers themselves, which, as call initiators, select an approved certification authority from which to request a certificate, and which, as call recipients, check with certification authorities to ensure that the certificates they receive were issued by the correct certification authority. Voice service providers use the digital certificates to indicate that they are trusted members of the ecosystem and their assertions to a calling party's identity should be accepted.

12. Under the current Governance Authority rules, a voice service provider must meet certain requirements to receive a certificate. Specifically, a voice service provider must have a current FCC Form 499A on file with the Commission, have been assigned an Operating Company Number (OCN), and have direct access to telephone numbers from the North American Numbering Plan Administrator (NANPA) and the National Pooling Administrator. The Governance Authority reviews this policy "at least on a quarterly basis," or as needed.

13. *Commission Action to Promote STIR/SHAKEN*. In 2017, the Commission released a *Notice of Inquiry* into STIR/SHAKEN, launching a broad examination of how to expedite its development and implementation. The Commission directed its expert advisory committee on numbering, the North American Numbering Council (NANC), to recommend "criteria by which a [Governance Authority] should be selected" and "a reasonable timeline or set of milestones for adoption and deployment" of STIR/SHAKEN. In its May 2018 report, the NANC made a number of recommendations regarding establishing and organizing a governance system and promoting STIR/SHAKEN implementation, which Chairman Pai then accepted. In November 2018, Chairman Pai sent letters to 14 major voice service providers urging them to implement a robust caller ID authentication framework by the end of 2019, asking providers for

specific details on their progress and plans. In June 2019, the Commission adopted a *Declaratory Ruling and Third Further Notice of Proposed Rulemaking* (84 FR 29387, June 24, 2019, and 84 FR 29478, June 24, 2019) that proposed and sought comment on mandating implementation of STIR/SHAKEN in the event that major voice service providers did not voluntarily implement the framework by the end of 2019. Commission staff closely tracked the implementation progress of major voice service providers. In December 2019, Congress enacted the TRACED Act, which contains numerous provisions directed at addressing robocalls, including through implementation of STIR/SHAKEN. Among other provisions regarding caller ID authentication, the TRACED Act directed the Commission to require, no later than 18 months from enactment, all voice service providers to implement STIR/SHAKEN in the IP portions of their networks and implement an effective caller ID authentication framework in the non-IP portions of their networks.

14. In March of this year, we released the *First Caller ID Authentication Report and Order and FNPRM* in which we adopted rules requiring voice service providers to implement the STIR/SHAKEN caller ID authentication framework in the IP portions of their networks by June 30, 2021. We also proposed and sought comment on requirements to strengthen STIR/SHAKEN to implement the TRACED Act. First, we proposed to extend the STIR/SHAKEN implementation mandate to intermediate providers and require them to both pass authenticated caller ID information unaltered and to authenticate unauthenticated calls they receive. Second, turning to TRACED Act implementation, we proposed to grant an extension for compliance with the implementation mandate for certain categories of voice service providers, specifically small voice service providers and voice service providers that materially rely on non-IP networks. Third, we proposed to require voice service providers using non-IP technology, which cannot support STIR/SHAKEN, to either (i) upgrade their networks to IP to enable STIR/SHAKEN implementation or (ii) work to develop non-IP caller ID authentication technology. Fourth, we proposed to implement a process, as directed by the TRACED Act, pursuant to which voice

service providers may become exempt from the STIR/SHAKEN implementation mandate if we determine that they have achieved certain implementation benchmarks. Fifth, we proposed to prohibit voice service providers from imposing additional line item charges on consumer and small business subscribers for caller ID authentication. Sixth, we sought comment on how to address consumer confusion or competition issues related to call labeling. We are continuing to monitor when and how terminating voice service providers label calls based on STIR/SHAKEN information and will not act on this matter at this time. Finally, we sought comment, as directed by the TRACED Act, on whether and how to modify our policies regarding access to numbering resources to help reduce illegal robocallers' access. We are continuing to review the record regarding access to numbering resources and will not act on this matter at this time.

15. *Implementation Progress*. As reported previously, major voice service providers fell into one of three categories regarding their implementation progress by the end of 2019: (1) voice service providers that upgraded their networks to support STIR/SHAKEN and began exchanging authenticated traffic with other voice service providers; (2) voice service providers that upgraded their networks to support STIR/SHAKEN but had not yet begun exchanging authenticated traffic with other voice service providers; and (3) voice service providers that had achieved limited, if any, progress towards upgrading their networks to support STIR/SHAKEN. Since the end of 2019, several major voice service providers have announced further progress in STIR/SHAKEN implementation. In February 2020, T-Mobile announced that it began exchanging authenticated traffic with Sprint, and in March 2020, Bandwidth announced that it has begun exchanging authenticated traffic with T-Mobile. In addition to the 14 major voice service providers discussed in detail in the *First Caller ID Authentication Report and Order and FNPRM*, other voice service providers and intermediate providers have made progress toward STIR/SHAKEN implementation as well. The Governance Authority reports that 34 voice service providers have been approved to participate in the STIR/SHAKEN framework through the governance system; 9 providers have completed the testing process and are finalizing their

approval; and 52 providers have begun registration and are in some stage of the testing process.

III. SECOND REPORT AND ORDER

16. In this document, we take the next steps to promote the widespread deployment of caller ID authentication technology and implement the TRACED Act. In the Report and Order, we first address the definitions and scope of several terms used in the TRACED Act. Next, we adopt rules on caller ID authentication in non-IP networks. We assess the burdens and barriers to implementation faced by various categories of voice service providers and adopt extensions to the STIR/SHAKEN mandate based on our assessment. We also establish the required robocall mitigation program that voice service providers with an extension must implement and elaborate on the annual reevaluation process for extensions required by the TRACED Act. We then adopt rules implementing the exemption mechanism established by the TRACED Act for voice service providers that meet certain criteria regarding early STIR/SHAKEN implementation. We prohibit voice service providers from imposing additional line item charges for call authentication technology. Finally, to avoid gaps in a call path that could lead to the loss of caller ID authentication information, we expand our STIR/SHAKEN implementation mandate to encompass intermediate providers.

A. TRACED Act Definitions and Scope

17. In the *First Caller ID Authentication Report and Order and FNPRM*, we adopted definitions of several terms used in the TRACED Act. Specifically, we adopted definitions of "STIR/SHAKEN authentication framework" and "voice service" that closely align with the statutory language enacted by Congress. To provide an opportunity for further refinement of the definitions we adopted, we sought comment in the *FNPRM* on whether to alter or add to them. We also proposed in the *FNPRM* to interpret "providers of voice service" on a call-by-call basis rather than a provider-by-provider basis in order to best effectuate Congressional direction. In other words, we proposed evaluating whether a specific entity is a voice service provider (i.e., "provider of voice service") within the meaning of the TRACED Act on the basis of the entity's

role with respect to a particular call, rather than based on the entity's characteristics as a whole. In this document, we reaffirm our definitions of "STIR/SHAKEN authentication framework" and "voice service," and adopt a rule codifying our proposed interpretation of "providers of voice service."

18. *Definition of "STIR/SHAKEN Authentication Framework."* The definition of "STIR/SHAKEN authentication framework" that we adopted in the *First Caller ID Authentication Report and Order and FNPRM* closely tracks the language Congress used in the TRACED Act. In the Report and Order, we defined "STIR/SHAKEN authentication framework" as "the secure telephone identity revisited and signature-based handling of asserted information using tokens standards." We did not receive any comments in the record seeking clarification, so we reaffirm the definition we adopted previously.

19. *Definition of "Voice Service."* We next reaffirm the definition of "voice service" that we adopted in the *First Caller ID Authentication Report and Order and FNPRM*. Specifically, we defined "voice service" as a service "that is interconnected with the public switched telephone network and that furnishes voice communications to an end user," and which includes "without limitation, any service that enables real-time, two-way voice communications, including any service that requires [IP]-compatible customer premises equipment . . . and permits out-bound calling, whether or not the service is one-way or two-way voice over [IP]." The definition we adopted is identical to the language Congress included in the TRACED Act. We explained in the *First Caller ID Authentication Report and Order and FNPRM* that, based on the definition of "voice service" we adopted, our STIR/SHAKEN rules apply to "all types of voice service providers—wireline, wireless, and Voice over Internet Protocol (VoIP) providers," including both two-way and one-way interconnected VoIP providers. And we clarified that voice service providers which lack control over the network infrastructure necessary to implement STIR/SHAKEN are not subject to our implementation requirements. Commenters that address the issues nearly unanimously support our definition and interpretation of "voice

service," though several commenters seek further clarification. Noble Systems argues that the Commission should interpret our definition of "voice service" broadly to encompass intermediate providers. We maintain our belief that the statutory language of the TRACED Act forecloses this interpretation by specifying that "voice service" means a service that "furnishes voice communications to an end user."

20. First, NCTA and CenturyLink advocate for us to interpret our rules to apply to "over-the-top (OTT) service that possess technical control over the origination of calls on their platforms." No commenter opposed these requests. We reiterate our belief that for STIR/SHAKEN to be successful, every service provider capable of implementing the framework must participate. We therefore conclude that to the extent a provider of OTT service provides "voice service," and has control of the relevant network infrastructure to implement STIR/SHAKEN, it is subject to our rules.

21. NCTA further encourages us to revise the current definition of "interconnected VoIP" found in § 9.3 of our rules in order to "harmonize" it with our caller ID authentication regulations. Section 9.3 generally limits "interconnected VoIP service" to *two-way* interconnected VoIP and only includes one-way VoIP as "interconnected VoIP" in the context of the Commission's 911 obligations. We understand the definition of "voice service" that Congress adopted in the TRACED Act to encompass both two-way and one-way interconnected VoIP. Because we rely on the statutory term "voice service" and because the meaning of that term is not limited by the definition of "interconnected VoIP" in § 9.3 of our rules, we see no reason to revisit of the definition of interconnected VoIP in § 9.3 in this proceeding.

22. Second, Microsoft argues that the definition of "voice service" should be read to exclude inbound-only VoIP service. Microsoft argues that this service is outside the scope of the STIR/SHAKEN standards, and that the reference to service that "permits out-bound calling" in the TRACED Act definition precludes application of our requirement to inbound-only VoIP service. We disagree. We understand the TRACED Act—which defines "voice service" to mean

"*any service* that is interconnected with the public switched telephone network and that furnishes voice communications to an end user" and includes, "*without limitation,* any service that enables real-time, two-way voice communications, including any service that . . . permits out-bound calling"—to establish a broad concept of voice service. We read the phrase "without limitation" as indicating that the subsequent phrase "permits out-bound calling" is not a limitation on the initial, general definition of "voice service," which encompasses in-bound VoIP. Similarly, in the context of our Truth in Caller ID rules, we interpreted the term "interconnected" as used in a substantially similar definition of "voice service" in the RAY BAUM's Act to include any service that allows voice communications either to or from the public switched telephone network (PSTN), regardless of whether inbound and outbound communications are both enabled within the same service. Because our STIR/SHAKEN rules impose obligations on both the originating and terminating side of a call, we believe that this broad reading of "interconnected" is also appropriate here. Further, reaching in-bound VoIP advances the purposes of the TRACED Act and widespread caller ID authentication. Our rules, consistent with the ATIS standards, require a voice service provider terminating a call with authenticated caller ID information to verify that information according to the STIR/SHAKEN framework. We thus reject Microsoft's argument that reaching in-bound VoIP is unnecessary because the standards comprising STIR/SHAKEN do not assign actions to be taken when terminating a call.

23. *Definition of "Providers of Voice Service"—Call-by-Call Basis.* Congress directed many of the TRACED Act caller ID authentication requirements to "providers of voice service." We proposed in the *First Caller ID Authentication Report and Order and FNPRM* to interpret "providers of voice service" on a call-by-call—rather than entity-by-entity—basis. Under this interpretation, a provider of voice service is not subject to TRACED Act requirements for all services simply because some of its services fall under the definition of "voice service." Instead, only those services that meet the TRACED Act definition of "voice service" are subject to TRACED Act obligations. We adopt our proposal. Both commenters that addressed the issue

support our proposal. We find that the call-by-call approach best fits the TRACED Act's structure because it gives meaning to Congress's inclusion of a definition for "voice service" and because it best comports with the TRACED Act's allocation of duties on the basis of call technology, *e.g.*, differentiating duties between calls over IP and non-IP networks.

B. Caller ID Authentication in Non-IP Networks

24. The TRACED Act directs us, not later than June 30, 2021, to require voice service providers to take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of their networks. Given the large proportion of TDM-based networks still in use, we expect a significant number of calls to be outside the STIR/SHAKEN authentication framework in the near term. In light of this, it is critically important that we take strong action to address the issue of caller ID authentication in non-IP networks. To that end, we interpret the TRACED Act's requirement that a voice service provider take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of its network as being satisfied only if the voice service provider is actively working to implement a caller ID authentication framework on those portions of its network. A voice service provider satisfies this obligation by either (1) completely upgrading its non-IP networks to IP and implementing the STIR/SHAKEN authentication framework on its entire network, or (2) working to develop a non-IP authentication solution. We adopt rules accordingly, and find that this approach best balances our goal of promoting the IP transition while simultaneously encouraging the development of a non-IP authentication solution for the benefit of those networks that cannot be speedily or easily transitioned. By adopting rules that are not overly burdensome, we leave voice service providers free to prioritize transitioning to IP, and we strongly encourage voice service providers to take advantage of this opportunity to do so.

25. In the *First Caller ID Authentication Report and Order and FNPRM*, we proposed that a voice service provider satisfies the "reasonable measures" requirement under

section 4(b)(1)(B) of the TRACED Act if it is able to provide us, upon request, with documented proof that it is participating, either on its own or through a representative, as a member of a working group, industry standards group, or consortium that is working to develop a non-IP solution, or actively testing such a solution. We explained that this proposal was consistent with our proposed approach to assessing whether a voice service provider is making "reasonable efforts" to develop a caller ID authentication protocol in the context of determining whether to limit or terminate an extension of compliance granted under section 4(b)(5)(B) for non-IP networks. We adopt a new rule reflecting this proposal and clarify its specific requirements.

26. Under our rule, a voice service provider satisfies its obligations if it participates through a third-party representative, such as a trade association of which it is a member or vendor. While our proposal did not include mention of trade associations or vendors, we agree with CCA that it would be best to broaden the scope of this requirement by including such representatives within the bounds of our requirement. Some industry groups have already established working groups dedicated to examining potential non-IP call authentication technologies. Allowing for such representatives will reduce the burden of this obligation on individual voice service providers and minimize the potential negative impact of broad and inexpert participation identified in the record, while ensuring that all voice service providers remain invested in developing a solution for non-IP caller ID authentication. A wider range of efforts will encourage a greater number of industry partnerships, increasing resource and information sharing and speeding the development of a non-IP solution.

27. We expect the benefits of this approach to be numerous, and the costs to voice service providers comparatively small. While some commenters provided estimates of the cost of replacing their non-IP networks, none provided estimates of the cost of working to develop a caller ID authentication solution for non-IP networks. Given that our firm but flexible approach permits voice service providers to satisfy this obligation by participating either on their own or through a representative, as members of a working group or consortium that is working to

develop or actively testing a non-IP solution, we expect that any related compliance costs will be quite limited. By comparison, the benefits of voice service providers either upgrading their non-IP networks to IP to support STIR/SHAKEN or working to develop a caller ID authentication solution for non-IP networks will be considerable, not only in the less tangible benefits they will have for consumers by reducing the waste and frustration resulting from illegal robocalls, but in terms of actual monetary savings. Indeed, as we found in the *First Caller ID Authentication Report and Order and FNPRM*, the monetary benefits of STIR/SHAKEN are likely to be in the billions of dollars. The greater the number of voice service providers that implement an effective caller ID authentication framework—either by upgrading their non-IP networks to IP and implementing STIR/SHAKEN, or by developing and implementing an effective non-IP solution—the more effective these frameworks will be in combatting illegal robocalls, and the more of the expected benefits will be realized. Thus, the rules we adopt in this document will help achieve these savings while simultaneously minimizing the cost of compliance.

28. We disagree with ATIS's contention that we should not adopt rules governing non-IP caller ID authentication until the joint ATIS/SIP Forum IP-NNI Task Force concludes its work investigating the viability of non-IP caller ID authentication frameworks. Given that this task force is precisely the kind expressly contemplated, and indeed, mandated, by our order in this document, we see no reason to delay these rules. Indeed, the Task Force's existence is confirmation that we have construed the "reasonable measures" standard in a manner that appropriately dovetails with current industry efforts to develop a non-IP solution. Further, the rules we adopt in this document are required by Congressional direction to mandate voice service providers to take "reasonable measures" to implement a non-Internet Protocol no later than June 30, 2021; we have no discretion to wait until a given task force has concluded its work to adopt rules.

29. Although CTIA argues that requiring voice service providers to participate in industry standards groups committed to developing or actively testing a non-IP solution "may

not improve the development" of such solutions, and would in fact "divert resources from STIR/SHAKEN deployment and other robocalls mitigation efforts," it offers no alternative interpretation of the "reasonable measures" standard mandated by Congress in the TRACED Act. We must impose a meaningful mandate to fulfill Congress's direction to require "reasonable measures to implement" a non-IP caller ID authentication solution. Requiring voice service providers that choose not to upgrade their non-IP networks to IP to contribute to groups and organizations that are working to test or develop a non-IP solution strikes a balance between promoting caller ID authentication solutions for TDM networks, as required by the TRACED Act, and leaving resources free to invest in IP networks. By allowing participation through a working group, consortium, or trade association, we allow voice service providers to efficiently pool their expertise and resources with the goal of not replicating one another's efforts and more efficiently developing a non-IP solution. We therefore are not convinced by CTIA's arguments that the requirement we adopt will unduly stunt STIR/SHAKEN deployment or that voice service providers will have "few resources left to dedicate to industry standards groups."

30. We are likewise unconvinced by TransNexus's conclusory claim that participating in a working group would not constitute a "reasonable effort" to implement an effective caller ID authentication framework on non-IP networks. Contributing to an industry-led body dedicated to pooling expertise and resources in the hopes of developing and/or testing non-IP solutions is a reasonable and efficient strategy for encouraging the creation and deployment of such solutions.

31. *Out-of-Band STIR.* We decline to mandate out-of-band STIR for non-IP networks. Out-of-band STIR is a proposed non-IP solution whereby caller ID authentication information is sent across the Internet, *out-of-band* from the call path. Commenters have widely divergent views as to the viability of out-of-band STIR as a method of effective caller ID authentication in non-IP networks. While a handful advocate for the implementation of out-of-band STIR as the best method of ensuring effective call authentication in non-IP networks, with

Neustar even claiming that this solution should be widely available in advance of the June 30, 2021 implementation deadline, many others contend that out-of-band STIR is not yet a viable solution. Comcast claims that out-of-band STIR is an untested, time-consuming, and costly solution that would require the re-creation of multiple network functions in parallel to IP networks. Given the undeniably sharp divide between commenters and the absence of sufficient testing and implementation to demonstrate the viability of out-of-band STIR as an industrywide solution, we find that it is not possible to conclude, based on the record before us, that out-of-band STIR is an effective non-IP solution. We find that significant industry consensus is an important predicate to deeming a non-IP solution "effective," given that cross-network exchange of authenticated caller ID information is a central component to caller ID authentication. Thus, we cannot at this time mandate adoption of out-of-band STIR by voice service providers in the non-IP portions of their networks. At the same time, we observe that opponents of this technology have offered no meaningful alternative solutions. To those that would oppose this possible solution without mention of an alternative, we take this opportunity to note that standards work requires both constructive input and compromise on the part of all parties and stakeholders.

32. *Effective Non-IP Caller ID Authentication Framework.* As we explain in the context of the extension of the implementation deadline for certain non-IP networks, we will continue to evaluate whether an effective non-IP caller ID authentication framework emerges from the ongoing work that we require. Consistent with that section, we will consider a non-IP caller ID authentication framework to be effective only if it is: (1) fully developed and finalized by industry standards; and (2) reasonably available such that the underlying equipment and software necessary to implement such protocol is available on the commercial market. An effective framework would exist when the fundamental aspects of the protocol are standardized and implementable by industry and the equipment and software necessary for implementation is commercially available. If and when we identify an effective framework, we expect to revisit

our "reasonable measures" requirement and shift it from focusing on development to focusing on implementation. We encourage voice service providers and others to put forward a framework they view as effective for our consideration. We also will continue to monitor progress in developing a non-IP authentication solution and may revisit our approach to the TRACED Act's "reasonable measures" requirement if we find that industry has failed to make sufficient progress in either transitioning to IP or developing a consensus non-IP authentication solution. We stand ready to pursue additional steps to ensure more fulsome caller ID authentication in non-IP networks, including by revisiting our non-prescriptive development-based approach if needed.

33. *Legal Authority*. We find authority for these rules under section 4(b)(1)(B) of the TRACED Act. That section expressly directs us to obligate voice service providers to take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of their networks and is a clear source of authority for these non-IP obligations.

34. We also conclude that section 251(e) of the Communications Act of 1934, as amended (the Act), provides additional independent authority to adopt these rules. Section 251(e) provides us "exclusive jurisdiction over those portions of the North American Numbering Plan (NANP) that pertain to the United States." Pursuant to this provision, we retain "authority to set policy with respect to all facets of numbering administration in the United States." Our exclusive jurisdiction over numbering policy enables us to act flexibly and expeditiously with regard to important numbering matters. When bad actors unlawfully falsify or spoof the caller ID that appears on a subscriber's phone, they are using numbering resources to advance an illegal scheme. Mandating that voice service providers take "reasonable measures" to deploy an effective caller ID authentication framework in the non-IP portions of their networks will help to prevent the fraudulent exploitation of NANP resources by permitting those providers and their subscribers to identify when caller ID information has been spoofed. Section 251(e) thus grants us authority to mandate that voice service providers take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of their networks in order to

prevent the fraudulent exploitation of numbering resources. Moreover, as the Commission has previously found, section 251(e) extends to "the use of . . . unallocated and unused numbers"; it thus gives us authority to mandate that voice service providers implement an effective caller ID authentication framework to address the spoofing of unallocated and unused numbers.

35. Finally, we find authority under the Truth in Caller ID Act. Congress charged us with prescribing regulations to implement that Act, which made unlawful the spoofing of caller ID information "in connection with any voice service or text messaging service . . . with the intent to defraud, cause harm, or wrongfully obtain anything of value." Given the constantly evolving tactics by malicious callers to use spoofed caller ID information to commit fraud, we find that the rules we adopt in this document are necessary to enable voice service providers to help prevent these unlawful acts and to protect voice service subscribers from scammers and bad actors. Thus, section 227(e) provides additional independent authority for these rules.

C. Extension of Implementation Deadline

36. The TRACED Act includes two provisions for extension of the June 30, 2021 implementation date for caller ID authentication frameworks. First, the TRACED Act states that we "may, upon a public finding of undue hardship, delay required compliance" with the June 30, 2021 date for caller ID authentication framework implementation for a "reasonable period of time." Second, we "shall grant a delay of required compliance" with the June 30, 2021 implementation date "to the extent that . . . a provider or class of providers of voice services, or type of voice calls, materially relies on a non-[IP] network for the provision of such service or calls" "until a call authentication protocol has been developed for calls developed over non-[IP] networks and is reasonably available."

37. Under either extension provision, an extension may be provider-specific or apply to a "class of providers of voice service, or type of voice calls." We must annually reevaluate any granted extension for compliance. When granting an extension of the implementation deadline under either provision, we must require impacted voice service providers to "implement

an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider."

38. Based on these directives and for the reasons discussed below, we grant the following extensions from implementation of caller ID authentication: (1) a two-year extension to small, including small rural, voice service providers; (2) an extension to voice service providers that cannot obtain a certificate due to the Governance Authority's token access policy until such provider is able to obtain a certificate; (3) a one-year extension to services scheduled for section 214 discontinuance; and (4) as required by the TRACED Act, an extension for the parts of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls until a solution for such calls is reasonably available. If at any point after receiving an extension a voice service provider no longer meets the extension criteria set for in this *Second Report and Order*, the extension will terminate. Upon termination of an extension, a voice service provider will be required to comply with our STIR/SHAKEN implementation mandate immediately. We further direct the Wireline Competition Bureau (Bureau) to reevaluate extensions annually, and we require any voice service provider that receives an extension to implement and certify that it has implemented a robocall mitigation program by June 30, 2021.

1. Assessment of Burdens and Barriers to Implementation and Extensions for Undue Hardship

39. The TRACED Act grants us the discretion to extend a voice service provider's obligation to comply with the June 30, 2021 caller ID authentication implementation mandate upon a public finding of undue hardship. It states that the extension may be "for a reasonable period of time . . . as necessary . . . to address the identified burdens and barriers." In connection with our determination of whether to grant an extension, the TRACED Act specifically directs us, not later than December 30, 2020 "and as appropriate thereafter," to assess any burdens and barriers to implementation of caller ID authentication technology by (1) voice service providers

that use time-division multiplexing network technology (TDM), a non-IP network technology; (2) small voice service providers; and (3) rural voice service providers. It further directs us to assess burdens and barriers created by the "inability to purchase or upgrade equipment to support the call authentication frameworks . . . or lack of availability of such equipment." The TRACED Act does not require us to grant undue hardship extensions to the categories of entities for which we must evaluate burdens and barriers to implementation, nor does it limit us to granting undue hardship extensions to entities within the categories for evaluation that it identifies. Based upon our review of the record, including our evaluation of burdens and barriers to implementation by certain categories of entities as directed by the TRACED Act, we grant extensions to: (1) small, including small rural, voice service providers; (2) voice service providers that cannot obtain the certificate necessary for STIR/SHAKEN; and (3) services subject to a discontinuance application. We decline to grant requested extensions for non-IP services, for larger rural voice service providers, due to equipment unavailability, for enterprise calls, for intra-network calls, or due to compatibility issues.

40. *Extension for Small Voice Service Providers*. The TRACED Act specifically directs us to evaluate whether to grant an extension based on undue hardship for small voice service providers. In the *First Caller ID Authentication Report and Order and FNPRM*, we proposed granting a one-year implementation extension due to undue hardship for small, including small rural, voice service providers. After reviewing the record, we grant a two-year extension for small voice service providers, which we define as those with 100,000 or fewer voice subscriber lines.

41. The record reflects that a barrier to STIR/SHAKEN implementation for small voice service providers is the substantial cost, despite resource constraints, to implement STIR/SHAKEN. For instance, according to CTIA, "many small providers face financial and resource constraints that other providers do not" as "[s]mall providers are driving toward the mandate deadline, but with fewer employees and smaller budgets, they may require more time to

transition to STIR/SHAKEN." Small voice service providers must also balance limited resources and expenses with other required technology transitions. Most recently, commenters explain that the COVID-19 pandemic has monopolized substantial available resources, increasing the burden on small voice service providers.

42. Relatedly, the record demonstrates that equipment availability issues specifically impact small voice service providers. Such providers rely on third-party vendor solutions, particularly software solutions, to implement STIR/SHAKEN, and these solutions may be prohibitively expensive for some small voice service providers. For instance, WISPA asserts that "[s]ome vendor's minimum fees could exceed a small provider's entire voice revenues." WTA agrees that the upfront expenses "could cause a budget shortage for small providers that have a limited, set multi-year budget that is already dedicated to new deployments, staff, etc." Further, ACA Connects expresses concern over a lack of transparency regarding the costs and relative advantages of available vendor solutions as its smaller voice service provider members, with limited budgets, must carefully apportion funds for STIR/SHAKEN deployment. Indeed, small voice service providers report they have "been quoted annual rates from different vendors that range from the low five figures to the low six figures, not including any upfront costs to install the solution," with no explanation for the rate disparity. The record reflects that as medium and large voice service providers start to widely deploy STIR/SHAKEN, new and improved solutions will emerge, increasing competition among vendors and decreasing costs. In addition, multiple commenters contend that small voice service providers are unable "to procure ready-to-install solutions" from a variety of vendors "on the same timeframe as the nation's largest voice service providers." According to NTCA, its members "are typically 'at the mercy' of vendors that respond to the larger operator community muc[h] faster, likely based on the latter's market share and buying power." As a result, timing and availability of these vendor solutions may be out of the control and reach of small voice service providers. Further, commenters contend that these vendor solutions remain at an early stage of development and "far

from ‘ready to install’ solutions.”

43. We are convinced by this record that an extension is appropriate for small voice service providers. The record largely supports our proposal for an implementation extension for small voice service providers, and we agree with these commenters that an extension is warranted to allow small providers sufficient time to address challenges such as equipment cost and availability. For instance, according to ACA Connects, NTCA, WISPA, and WTA, vendor costs may be prohibitively expensive for small voice service providers and could result in budget shortages. Additional time will allow voice service providers confronted with budget shortages to spread costs over a longer time horizon. Further, small voice service providers claim vendor solutions are still in nascent stages of development, and an extension will allow vendors that work with small voice service providers more time to develop solutions and offer those solutions at a lower cost as the market matures. Some small voice service providers also describe the inability to exchange traffic at non-IP interconnection points as a barrier to the exchange of calls with authenticated caller ID information after implementation of STIR/SHAKEN. In addition, to the extent that it uses TDM technology, a small voice service provider must contend with the associated technical and resource constraints to implementation. We address these issues separately.

44. Transaction Network Services and AT&T contend that we should not grant a blanket extension for small voice service providers. These commenters claim that such an extension would be overinclusive because not all small voice service providers face identical hardships, and allege that illegal robocalls may originate from these providers. We disagree. The overwhelming record support persuades us that small voice service providers, as a class, face undue hardship, and supports the need for a blanket implementation extension for such providers to give them the necessary time to implement STIR/SHAKEN. The TRACED Act also identifies small voice service providers as a class for which the Commission should assess burdens and barriers to implementation. Further, as ACA Connects contends, granting

extensions on a case-by-case basis for small voice service providers would "inundate the Commission with extension requests from a multitude of small providers, many of them presenting evidence of the same or similar implementation burdens" and "consume funds that would be better spent working towards implementation of STIR/SHAKEN." We do not find that this extension will unduly undermine the effectiveness of STIR/SHAKEN. As small voice service providers account for only a small percentage of voice subscribers, an extension covering these providers will account for the unique burdens they face while ensuring that many subscribers benefit from STIR/SHAKEN. Further, the prevalence of STIR/SHAKEN will encourage small voice service providers that can afford to do so to implement the framework as soon as possible to provide the protections it offers to their subscribers. And small voice service providers—like all providers subject to an extension—are obligated to implement a robocall mitigation program to combat the origination of illegal robocalls during the course of the extension.

45. We conclude that the extension we grant should run for two years, subject to possible extension pursuant to the evaluation discussed below. Multiple commenters advocated for an extension longer than one year. For instance, WISPA and Atheral contend that small voice service providers require an extension of at least two years beyond the implementation deadline to "budget for and absorb the cost of needed upgrades" and to "allow for the development of vendor solutions and reduction in cost to more affordable levels as volume scales." We expect this extension for small voice service providers will drive down implementation costs by allowing these providers to benefit from a more mature market for equipment and software solutions necessary to implement STIR/SHAKEN. Small voice service providers have also filed estimates of the cost of implementing STIR/SHAKEN on their networks. The additional implementation time will allow these providers to spread the cost of implementation across a longer time horizon. We find that an implementation deadline of two-years allows for sufficient time—but no more than necessary—for small voice service providers

to meet the challenges of implementing STIR/SHAKEN on their networks. Our guiding principle in setting this deadline is to achieve ubiquitous STIR/SHAKEN implementation to combat the scourge of illegal caller ID spoofing as quickly as possible. This extension should also ease the additional burdens placed on small voice service providers by the COVID-19 pandemic, which has consumed significant resources.

46. We decline at this time NTCA's requests to tie an implementation extension until June 30, 2023 to "the vendor community delivering solutions in 2020," and to grant additional implementation time for small voice service providers "unable to obtain vendor solutions by the end of 2020." NTCA contends that the two-year extension may be insufficient to resolve the issues presented by the lack of IP interconnection if vendor solutions are not available to small voice service providers by the end of 2020. We separately address the issue of non-IP interconnection. In the interest of promoting ubiquitous STIR/SHAKEN implementation, we decline at this time to grant a longer extension for small voice service providers that may face continued implementation challenges in the future. We find that a longer extension would discourage the swift development of effective vendor solutions and slow the deployment of STIR/SHAKEN to the detriment of consumers. We also find that a longer extension would unnecessarily rely on speculation about marketplace realities several years from now. The Bureau may grant a further extension if it determines such an extension is appropriate in its annual reevaluation.

47. Finally, we establish that, as proposed in the *First Caller ID Authentication Report and Order and FNPRM*, a provider is a "small provider[] of voice service" for purposes of this extension if it has 100,000 or fewer voice subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of a provider's affiliates). In the *First Rural Call Completion Order* (78 FR 76218, Dec. 17, 2013), the Commission determined that the 100,000-subscriber-line threshold ensured that many subscribers would continue to benefit from our rules while also limiting the burden on smaller

voice service providers. Similarly, we find that, in the caller ID authentication context, limiting the implementation extension for small voice service providers to those that have 100,000 or fewer voice subscriber lines balances the needs of these providers and the importance of widespread and effective STIR/SHAKEN implementation. We received support in the record for this definition of "small providers of voice service."

48. We decline at this time USTelecom's post-circulation request to exclude voice service providers within the 100,000-subscriber-line threshold that "originate a disproportionate amount of traffic relative to their subscriber base, namely voice service providers that serve enterprises and other heavy callers through their IP networks." While we see value in the policy goals that underlie USTelecom's request, implementing its suggestion would require a difficult line-drawing exercise. USTelecom did not offer any support for its proposed criteria to identify parties that originate a disproportionate amount of traffic, nor are we able to identify criteria in the limited time available in which we have confidence. We are open to revisiting this issue should we determine that the extension creates an unreasonable risk of unsigned calls from a specific subset of small voice service providers.

49. *Extension for Voice Service Providers That Cannot Obtain a Certificate.* In the *First Caller ID Authentication Report and Order*, we acknowledged the concerns raised by Cloud Communications Alliance regarding whether all voice service providers are able to obtain the certificates used for the intercarrier exchange of authenticated caller ID information under the Governance Authority's current policies. And in the *FNPRM*, we asked whether we should grant an implementation extension for any other voice service providers or classes of voice service providers, or types of calls. In response, commenters advocated for an extension for voice service providers that cannot obtain a certificate because they are ineligible to file FCC Form 499A, obtain an Operating Company Number, or obtain direct access to telephone numbers—each of which is a prerequisite to obtaining a certificate under current Governance Authority policy.

50. Because it is impossible for a service provider to participate in STIR/SHAKEN without access to the required certificate and because some voice service providers are unable to obtain a certificate at this time, we determine that a limited extension is necessary. Multiple commenters contend that the Governance Authority's policy excludes voice service providers that lease numbers rather than obtain them directly from NANPA. In particular, one-way VoIP voice service providers have no means to obtain direct access to numbers, so they cannot obtain the certificate necessary to comply with their duty to implement STIR/SHAKEN. Only carriers and interconnected VoIP providers may obtain direct access to telephone numbers. Therefore, we grant an extension to voice service providers that cannot obtain a certificate due to the token access policy. We grant this extension until it is feasible for a provider to participate in STIR/SHAKEN due either to the possibility of compliance with the Governance Authority policy or a change in the Governance Authority policy. We recognize that a voice service provider may not be able to immediately come into compliance with its caller ID authentication obligations after it becomes eligible to receive a certificate, and we will not consider a voice service provider that diligently pursues a certificate once it is able to receive one in violation of our rules. PACE also requests that we determine whether a voice service provider subject to this extension may comply with our caller ID authentication requirements "by relying on a 3rd party service provider." In the absence of a more complete record to guide our decision, we decline to accept this request at this time. We expect the extension we establish will decrease costs by relieving such providers from the obligation to upgrade their networks until they can meaningfully participate in STIR/SHAKEN. We recognize that industry has made progress on resolving the gap between Governance Authority certificate access policies and the scope of duties we have established pursuant to the TRACED Act, and we continue to urge speedy resolution of these issues. We decline Noble Systems' request for us to direct the Governance Authority to "revisit its policies that were defined prior to passage of the TRACED Act" and "revisit the makeup of the [Governance Authority] membership in light of the broad scope of

"voice service" in the TRACED Act." In the *First Caller ID Authentication Report and Order and FNPRM*, we declined to intervene in or impose new regulations on the STIR/SHAKEN governance structure and maintain that position. We reiterate that because the Governance Authority is made up of a variety of stakeholders representing many perspectives, we have no reason to believe it will not operate on a neutral basis.

51. *Extension for Services Scheduled for Section 214 Discontinuance*. In the *First Caller ID Authentication Report and Order and FNPRM*, we also sought comment on whether to consider any additional categories of extensions. In response to AT&T's request, we grant a one-year extension based on undue hardship to cover services for which a provider has filed a pending section 214 discontinuance application on or before the June 30, 2021, STIR/SHAKEN implementation deadline. Verizon and CenturyLink advocate for removing discontinuance obligations that "require [voice service] providers to obtain permission prior to replacing TDM voice services with VoIP" to "help make network transitions to IP more straightforward and efficient." We decline to grant this request as it is outside the scope of the current proceeding. This extension will allow voice service providers time to either complete the discontinuance process and "avoid incurring unnecessary expense and burden to implement STIR/SHAKEN" for services "that are scheduled to sunset," or to implement STIR/SHAKEN for any such services that are not discontinued. We agree with AT&T that voice service provider resources "are better spent upgrading networks that will have the potential to reap the full benefits of the IP transition and STIR/SHAKEN." We expect that this extension will decrease costs by obviating the need to upgrade components of a voice service provider's network that will be sunset. We underscore that a one-year extension means that voice service providers have until June 30, 2022, to either discontinue the legacy service or implement STIR/SHAKEN if the service has not actually been discontinued, unless the provider obtains a waiver of this requirement for good cause shown. If we determine that a voice service provider filed a discontinuance application in bad faith to receive this extension, we will terminate the extension and take appropriate action.

52. *Voice Service Providers That Use TDM—An Extension Would Be Superfluous*. The TRACED Act specifically directs us to evaluate whether to grant an extension to voice service providers that use TDM network technology. The record reflects that a major barrier to implementation of a caller ID authentication framework for voice service providers that use TDM technology is the lack of a standardized caller ID authentication framework for non-IP networks. Because the STIR/SHAKEN framework is an IP-only solution, these voice service providers must expend substantial resources upgrading network software and hardware to be IP compatible in order to implement the only currently available standardized caller ID authentication solution. According to commenters, voice service providers that use TDM networks also face availability and cost issues regarding necessary equipment to upgrade the software and hardware to convert their networks to IP. Further, small or rural voice service providers that use TDM technology may have fewer resources and require additional time for transitioning their networks to IP technology. Multiple commenters agree that "[e]ven if a [voice service provider] has upgraded its own network to all-IP technology, if that [voice service provider] exchanges substantial traffic through legacy TDM tandems, such tandems will similarly present obstacles to STIR/SHAKEN deployment."

53. Although we proposed in the *First Caller ID Authentication Report and Order and FNPRM* to grant the same extension to voice service providers that use TDM technology under the undue hardship standard that we grant to providers that materially rely on non-IP technology, we conclude that a separate and identical extension is redundant and creates administrative duplication. We want to avoid granting two separate extensions, with associated filing and review requirements, that serve identical purposes. Because the TRACED Act includes a required extension for voice service providers that "materially rel[y]" on non-IP technology, we decline to grant a separate extension to voice service providers that use TDM technology under the undue hardship standard. This extension (1) applies to those parts of a voice service provider's network that materially rely on technology that cannot initiate, maintain,

and terminate SIP calls; (2) lasts "until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available"; and (3) may be terminated if the Commission determines that a voice service provider "is not making reasonable efforts to develop the call authentication protocol" for non-IP networks. Although AT&T contends that "an extension for TDM networks is independently warranted," it does not explain its position. In fact, AT&T concedes that "the extension outcomes are the same." We find the non-IP extension sufficiently addresses AT&T's concern that there is not yet a STIR/SHAKEN-equivalent solution for TDM networks. To the extent there is any lack of clarity, we confirm that TDM networks are included in the non-IP extension established below, and subject to its terms.

54. *Rural Voice Service Providers—A Separate Extension Is Unnecessary*. The TRACED Act specifically directs us to evaluate whether to grant an extension based on undue hardship to rural voice service providers. The record reflects that the burdens and barriers to STIR/SHAKEN implementation for rural voice service providers are often encompassed by those for small voice service providers or voice service providers that use non-IP network technology because these voice service providers also tend to be rural. To the extent rural voice service providers rely on non-IP technology, which is incompatible with STIR/SHAKEN, they encounter the burdens already described for such providers. Similarly, the rural voice service providers that describe specific burdens to implementation—such as availability of vendor solutions that may be prohibitively expensive with few reasonable alternatives—are small voice service providers. Although CTIA generally states that there are potential financial and resource constraints for larger rural voice service providers, it does not identify any specific implementation challenges faced by these providers. Indeed, at least one larger rural voice service provider, TDS Communications, a Wisconsin-based voice service provider that serves nearly 900 rural, suburban, and metropolitan communities throughout the United States, has begun to invest in STIR/SHAKEN deployment.

55. In the *First Caller ID Authentication Report and Order and FNPRM*, we sought

comment on our proposed view that it would be unnecessary to grant a separate implementation extension for rural voice service providers as the challenges faced by these providers are already addressed by the small voice service provider extension and the extension for voice service providers that materially rely on a non-IP network. After review of the record, we adopt our proposal and decline to adopt a separate extension for rural providers. While we decline to grant an extension to this class of voice service providers, a voice service provider that believes that it faces an undue hardship may submit a filing that details its specific circumstances. The majority of commenters in the record did not differentiate rural voice service providers from those that are small and referred to them interchangeably. As noted above, the rural voice service providers that called for an extension are themselves small voice service providers. NCTA contends that a dedicated extension for rural providers is "unnecessary" because "the vast majority of rural providers will qualify for the small provider extension" or the extension for voice service providers that rely on non-IP networks. We agree with NCTA that "there does not seem to be a strong basis for granting any form of relief" to rural voice service providers that do not qualify as small voice service providers. Further, TDS reports that it had completed work in 2019 to evaluate, select, and lab test a vendor solution to allow it to integrate STIR/SHAKEN into the IP portions of its network. Because one large rural voice service provider has already invested in STIR/SHAKEN deployment to best serve its customers, we expect that other similarly situated rural voice service providers have also begun or would be capable of having begun the implementation process. We conclude that it would be improper to reach a blanket finding of undue hardship for rural voice service providers because (1) the record does not show that larger rural providers face undue hardship; and (2) our separate finding of undue hardship for small voice service providers relieves small rural voice service providers of the obligation to implement, such that they will no longer face undue hardship for the duration of the extension. Further, an extension for rural voice service providers would not only be unnecessary, but also harmful to the goal of widespread implementation.

56. We also decline the request by CTIA and USTelecom for an extension for vaguely-defined "regional" voice service providers that do not fall within our 100,000 or fewer voice subscriber line threshold. CTIA only generally describes potential financial and resource constraints for these voice service providers, and neither commenter sufficiently defines this class of providers or explains why we should grant an extension on the basis of undue hardship to providers with the resources that are necessary for serving a large number of subscribers. We similarly decline the request by Madison Telephone Networks for an extension until 2024 or 2025 for rural providers in high cost areas to "relieve financial pressure." We decline to grant this extension as Madison Telephone Networks does not demonstrate why this is a unique class of providers requiring an extension of this length. Further, we expect the majority of these voice service providers are also small or materially rely on non-IP technology and therefore will be covered by either or both of those extensions. If a voice service provider in this category is not covered by an extension and requires additional time for STIR/SHAKEN implementation, it may file an individual petition requesting an extension, as discussed below.

57. *Equipment Availability—A Separate Extension Is Unnecessary.* In the *First Caller ID Authentication Report and Order and FNPRM*, we sought comment on Congress's direction to consider whether to grant a separate extension on the basis of "the inability to purchase or upgrade equipment to support the call authentication frameworks under this section, or lack of availability of such equipment." We conclude that our extension for small voice service providers adequately addresses challenges with regard to obtaining necessary equipment and that a separate or additional extension is unnecessary. As discussed above, the record reflects that equipment availability specifically impacts small voice service providers. This is not a surprise, as it is likely that larger voice service providers have the resources and negotiating leverage to obtain the equipment they need much more quickly than small providers. Granting an extension solely for equipment unavailability may discourage larger voice service providers from putting forward sufficient effort to obtain necessary equipment. Further, no commenter has

identified any specific equipment availability issue for large voice service providers—commenters merely speak in general terms. Granting an *ex ante* extension on this basis would introduce difficult line-drawing questions as to when equipment is "unavailable" for which the record does not suggest a solution and that are not necessary to resolve in light of the extension for small voice service providers. We note that under our rules any voice service provider—large or otherwise—that encounters a specific equipment availability issue may request a waiver of the deadline.

58. *Enterprise Calls—An Extension Would Be Counterproductive*. In the *First Caller ID Authentication Report and Order and FNPRM*, we sought comment on whether we should grant an extension for undue hardship for enterprise calls. We described the concerns of some commenters that the standards for attestation do not fully account for the situation where an enterprise subscriber places outbound calls through a voice service provider other than the voice service provider that assigned the telephone number. In such enterprise calling scenarios, commenters claimed, it would be difficult for an outbound call to receive A-level attestation because the outbound call "will not pass through the authentication service of the [voice] service provider that controls th[e] numbering resource." To provide A-level attestation, the voice service provider must be able to confirm the identity of the subscriber making the call, and that the subscriber is using its associated telephone number. The record developed in response to our *Further Notice* reflects challenges for voice service providers to attest to enterprise calls with A-attestation in this and other circumstances, meaning that such calls would be authenticated with B- or C-level attestation. Based on these challenges, some commenters argue that we should grant an extension in compliance with the STIR/SHAKEN implementation mandate for enterprise calls so that these calls will not receive caller ID authentication until industry standards groups resolve the enterprise issue, rather than receiving a lower level of attestation in the interim. We agree with the record opposition, and we decline to grant an implementation extension to enterprise calling cases.

59. First, we agree with those commenters that argue that an implementation extension may discourage the swift development of technical solutions for enterprise calls. Although commenters offer different perspectives on the timing of a solution that would allow enterprise calls to receive A-level attestation, the record reflects that industry is "working hard to achieve authentication with A-level attestation this year." It is our goal to encourage this work, rather than remove the beneficial incentive created by the STIR/SHAKEN mandate. We decline, however, to go so far as some commenters suggest and "[r]equir[e] the prompt finalization of standards that will enable voice providers that originate enterprise calls to provide an A-level attestation." As industry stakeholders, standards bodies, and the Governance Authority are actively working to finalize standards and solutions to complex enterprise calling cases, we do not wish to intervene in the process. At the same time, we continue to encourage—and expect—industry to promptly resolve the outstanding challenges for complex enterprise use cases and business models, and we will closely monitor progress on this issue.

60. We are also not persuaded by claims that authenticating enterprise calls with B- or C-level attestation poses a major problem. These commenters contend that enterprise calls without an A-level attestation may be blocked, mislabeled as potentially fraudulent, or lead to illegal robocallers authenticating their own calls. However, they fail to explain how the alternative—an enterprise call without authenticated caller ID information—is preferable to one that receives B- or C-level attestation. Cloud Communications Alliance addresses this question, but states only that "[i]t is difficult to answer this question in the abstract without knowing the call validation treatment of B or C level attestations." It adds that if voice service providers or the industry "only value an 'A' level attestation when deciding call treatment, while wholly discounting a lower level of attestation, the ability to sign with a B or C level attestation will be of little benefit, perhaps apart from providing information for trace back purposes." Notably, NCTA reports that "[i]n [its] members' experiences, partial ('B') attestation can be achieved more quickly than complete ('A') attestation for enterprise calls," and accordingly, partial

attestation is "a reasonable implementation approach in this context." Similarly, Hiya, an analytics company, commits that it "currently has no plans—nor is it aware of any plans by other parties in the industry—to either block calls or label them as potentially fraudulent solely due to lack of 'full' or 'A' level attestation." It also asserts "that voice service providers and analytics engines will not use attestation level as the sole determinant for reputation scoring of a caller," and instead, "attestation information is one of the many data points that inform analytics-driven call labeling and call blocking." Vonage contends that attestation may provide a "potentially" "dispositive data point," but fails to support this claim. Transaction Network Services also explains that "STIR/SHAKEN attestations—'good' or 'bad'—will not have the effects that some commenters suggest" as it "endeavors to incorporate STIR/SHAKEN attestations *as one factor in its analysis*" and "does not recommended making call-blocking decisions based on the failure of STIR/SHAKEN authentication." Indeed, we have previously stated that "a call-blocking program might block calls based on a combination of factors." In the *Third Call Blocking Report and Order* (85 FR 56530, September 14, 2020), we also explained that "[i]f the terminating voice service provider has identified that calls with 'A' attestation previously originating from that number are nevertheless illegal or unwanted based on reasonable analytics, [it] may block those calls despite the attestation level." Even assuming that calls with B- or C-level attestation will be treated meaningfully worse than calls without authenticated caller ID information—a conclusion that, again, is not substantiated by the record—concerns over the treatment of calls authenticated consistent with current STIR/SHAKEN standards does not amount to an undue hardship in the *implementation* of STIR/SHAKEN technology, which is the standard by which Congress directed us to evaluate undue hardship extension requests. In light of these conclusions and our and Congress's goal of ubiquitous STIR/SHAKEN implementation in IP networks, we will not grant an extension for enterprise calls.

61. *Intra-Network Calls—An Extension Would Be Counterproductive*. In the *First Caller ID Authentication Report and Order and FNPRM*, we established distinct authentication

requirements for inter-network calls and for intra-network calls. In the case of inter-network calls, an originating voice service provider must "authenticate caller [ID] information for all SIP calls it originates and that [it] will exchange with another voice service provider or intermediate provider." This duty applies only "to the extent technically feasible." In the *First Caller ID Authentication Report and Order and FNPRM* we specifically recognized this fact, explaining that "transmission of STIR/SHAKEN authentication information over a non-IP interconnection point is not technically feasible at this time." Because establishing trust between providers is not necessary for calls that transit a single network, we adopted a different obligation for intra-network calls that solely transit the network of the originating voice service provider. Specifically, in recognition of the fact that "certain components of the STIR/SHAKEN framework . . . are not necessary for calls that a voice service provider originates and terminates on its own network," we concluded a voice service provider satisfies its intra-network authentication obligation so long as it authenticates and verifies "in a manner consistent with the STIR/SHAKEN framework, such as by including origination and attestation information in the SIP INVITE used to establish the call."

62. A number of commenters that exchange all traffic with other providers through non-IP interconnection points—and thus have no obligation under our rules to implement STIR/SHAKEN with respect to inter-network calls—seek an extension from the intra-network authentication requirement. These voice service providers seek such relief because compliance requires network upgrades, and they would prefer to delay investing in these necessary upgrades until they are able to participate in STIR/SHAKEN both within their own network and with regard to calls exchanged with other voice service providers, which require many of the same upgrades.

63. We decline to grant the requested extension because we do not find that it rises to the level of undue hardship. Commenters favoring an extension contend that requiring them to invest in compliance solely as to intra-network calls would require unreasonably burdensome

network upgrades that, in their view, produce limited benefits. But these commenters fail to explain why implementation would be more burdensome for them than for other voice service providers. In fact, implementation maybe less costly because our standard for intra-network IP calls is only that they are authenticated "in a manner consistent with the STIR/SHAKEN framework" which does not require those upgrades necessary to enable cross-provider authentication and verification. The TRACED Act requires an assessment of burdens and barriers, not a cost-benefit analysis, and parties seeking an extension have failed to show that they face atypical burdens and barriers on the basis of the intra-network authentication requirement. We nonetheless note that the benefits of our intra-network requirement are greater than parties favoring an extension contend. As we have explained, STIR/SHAKEN implementation provides benefits to consumers even at the intra-network level. Specifically, implementing STIR/SHAKEN within a voice service provider's own network directly benefits consumers as it enables a voice service provider to authenticate all calls among its customers. To that end, we agree with commenters that while voice service providers work toward IP interconnection, "[t]here is no reason to deny consumers" the "immediate benefits" of authenticated caller ID information for calls on their voice service provider's own network. Further, the record reflects that many providers that face challenges regarding IP interconnection are small providers, to which we have granted a two-year extension in compliance with the STIR/SHAKEN mandate. Providers so situated will therefore have additional time to negotiate IP interconnection agreements before being subject to the intra-network mandates. Various commenters in the record argue that the Commission should more directly resolve the issue of non-IP interconnection. While we refrain from directly addressing the issue of non-IP interconnection in this Order, which focuses largely on completing TRACED Act implementation as to STIR/SHAKEN, we will continue to monitor the issue.

64. Further, granting such an extension would impede the progress of the IP transition and further delay STIR/SHAKEN implementation—contrary to our goal of ubiquitous

deployment of caller ID authentication technology. Atheral and WISPA request that we establish a waiver process for providers with non-IP interconnection points that need to upgrade media gateways in order to exchange SIP calls. We decline to establish a unique process in this context, as these parties do not explain why our existing procedures are insufficient. Parties that wish to seek a waiver are free to do so pursuant to our existing procedures. We agree with Comcast that it is essential to "encourage the IP transition by, among other things, adopting policies in this proceeding that induce providers to prioritize the implementation of IP-enabled call authentication through STIR/SHAKEN." Comcast proposes that we "consider[] a provider's efforts to transition to . . . IP-to-IP voice interconnection[] when determining whether to grant or renew a limited extension." Because we do not grant an extension for the inability to exchange traffic at IP-enabled interconnection points, we see no need to adopt this suggestion. As AT&T observes, an extension for intra-network calls of providers that do not interconnect in IP would "discourag[e] voice service providers from coming to a negotiated resolution and transitioning to IP" at the interconnection point. By denying this extension, we "increase the[] incentive to negotiate creative and commercially reasonable interconnection agreements" to ensure that customers receive STIR/SHAKEN benefits.

65. *Provider-Specific Extensions.* We decline at this time to grant any extensions to individual voice service providers. We recognize, as INCOMPAS and CenturyLink suggest, that some providers may face specific circumstances in all or part of their IP networks that constitute undue hardship. The Commission will be in a better position to evaluate those requests, however, in response to specific petitions that establish in detail the basis for the requested extension, rather than through establishing a general principle in response to the vague and general concerns about technology or compatibility issues that INCOMPAS and CenturyLink set forth. A voice service provider that believes that it faces an undue hardship within the meaning of the TRACED Act may file in this docket an individual petition requesting an extension. We direct the Bureau to seek comment on any such petitions and to issue an order determining

whether to grant the voice service provider an extension. We expect any voice service provider seeking an extension to file its request by November 20, 2020, and we direct the Bureau to issue a decision no later than March 30, 2021. We find it appropriate to direct the Bureau to issue provider-specific extension determinations by March 30, 2021, so that the Bureau has adequate time to seek comment on and consider timely-filed petitions and petitioners have adequate time, before the June 30, 2021, implementation deadline, to act in response to the Bureau's determination. Although we expect voice service providers to file extension requests by November 20, 2020, we note that parties seeking additional extensions after this date are free to seek a waiver of our deadline under § 1.3 of the Commission's rules. This is consistent with the TRACED Act's mandate that the Commission consider the burdens and barriers to implementation "as appropriate" beyond the 12-month period specified in the Act. Of course, in determining whether it is "appropriate" to consider such late-filed requests, we expect that the Commission will not look favorably on requests that rely on facts that could have been presented to the Commission prior to November 20, 2020 with reasonable diligence. Given the importance of widespread STIR/SHAKEN implementation, to be granted an extension a voice service provider must demonstrate in detail the specific undue hardships, including financial and resource constraints, that it has experienced and explain why any challenges it faces meet the high standard of undue hardship to STIR/SHAKEN implementation within the timeline required by Congress.

2. Extension for Certain Non-Internet Protocol Networks

66. Section 4(b)(5)(B) of the TRACED Act directs that "the Commission shall grant a delay of required compliance . . . for any provider or class of providers of voice service, or type of voice calls, only to the extent that such a provider or class of providers of voice service, or type of voice calls, materially relies on a non-[IP] network for the provision of such service or calls . . . until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available." In implementing this provision, we impose the same

obligations on voice service providers that receive the extension as we impose in the mandate requiring voice service providers to implement an effective caller ID authentication framework in the non-IP portions of their networks. We note that, along with the obligations we impose for recipients of the non-IP extension, such recipients are also subject to the robocall mitigation requirements shared by all other recipients of extensions. We find that doing so ensures that all voice service providers with non-IP network technology are subject to the same burdens and are working together to develop a non-IP solution as envisioned by the TRACED Act. We also find that such action most efficiently carries out the goals of protecting consumers from illegal robocalls on non-IP networks, and encourages a general transition to IP and the wider implementation of STIR/SHAKEN.

67. *Eligibility for this Extension.* Under the TRACED Act, we must grant an extension for voice service providers or types of voice calls that "materially rel[y] on a non-[IP] network." We interpret this provision to mean that those portions of a voice service provider's network that do not use SIP technology are eligible for an extension of the implementation deadline of June 30, 2021. The TRACED Act states that we shall grant this extension "under section 4(b)(5)(A)(ii)," which governs extensions granted upon a public finding of undue hardship. We interpret this clause to mean that undue hardship is presumed where a voice service provider materially relies on a non-IP network for the provision of such service or calls. We also interpret "until a call authentication protocol has been developed . . . and is reasonably available" to be a statutorily-defined "reasonable period of time" for the purposes of this extension. In the *First Caller ID Authentication Report and Order and FNPRM*, we proposed defining "non-[IP] network[s]" as those portions of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls. We adopt our proposal because we believe this to be a straightforward implementation of Congress's direction in the TRACED Act, which also provides that extensions may be voice service provider-specific or apply to a class of voice service providers or type of voice calls. In determining whether a voice

service provider or type of voice calls "materially relies" on such a non-SIP capable network, we proposed to interpret "material[]" to mean "important or having an important effect" and, consistent with our call-by-call interpretation of the TRACED Act, we proposed to read "reli[ance]" with reference to the particular portion of the network in question. We adopt these proposed interpretations, which received no opposition in the record, and we therefore consider reliance on a non-IP network as material if that portion of the network is incapable of using SIP. Comcast argues that we should refrain from "applying new regulatory mandates to the entire voice industry," and should instead "consider[] a provider's efforts to transition to IP . . . when determining whether to grant or renew a limited extension of the STIR/SHAKEN implementation deadlines." We decline to take this approach, as we believe the approach we take in this document—imposing a broad mandate and granting an extension where necessary—better comports with the TRACED Act's mandatory extension for providers that "materially rely" on non-IP technology. Put another way, if a SIP-incompatible portion of a voice service provider's network is used for the provision of voice service, that portion of the network is eligible for an extension of the implementation deadline. The record reflects support for this interpretation. After noting that our definition's scope is consistent with the concept of material reliance, AT&T suggests that we add to our definition of "non-[IP] network" "all 'TDM in the middle' services—that is, those utilizing TDM switching/transport as well as those exchanged over TDM interconnection points." We decline to do so because we are only obligated under the TRACED Act to provide extensions for originating and terminating voice service providers, and not intermediate providers. We also note that the rules we adopt in this document regarding intermediate providers only apply to networks which support SIP signaling. We acknowledge the concerns raised by AT&T and others regarding the prevalence of non-IP networks, and find that their prevalence only increases the importance of taking action to encourage widespread caller ID authentication across all networks while the IP transition is ongoing.

68. *Duration of Extension.* The TRACED Act directs that the non-IP extension shall

end once "a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available." We also note that the TRACED Act grants us the authority to limit or terminate any granted non-IP extension if we determine that a voice service provider "is not making reasonable efforts to develop" a caller ID authentication protocol for non-IP networks. As noted later, we interpret "reasonable efforts" to mean that a voice service provider is participating, either on its own, in concert with a vendor, or through a representative, as a member of a working group, industry standards group, consortium, or trade association that is working to develop a non-IP solution, or actively testing such a solution. In determining whether a caller ID authentication protocol meets this standard, we adopt the test proposed by Alaska Communications, with some modifications. Consistent with Alaska Communications' proposal, we conclude that a caller ID authentication protocol "has been developed" if we determine that the protocol is fully developed and finalized by industry standards. By "fully developed" and "finalized" we do not require that the protocol must have achieved a status whereby no future development or progress is possible. Under that interpretation, the STIR/SHAKEN framework itself would not meet this standard. Instead, our standard does not foreclose the possibility of further development and improvement, but would only determine a protocol has been developed if at least all fundamental aspects of the protocol which enable its effectiveness are standardized by industry, and the protocol is implementable by voice service providers. We agree with commenters that such a protocol must be standards-based and ready for implementation. Although some commenters advocate for mandating out-of-band STIR, we find that this solution is not yet standardized. We thus conclude that, at this time, no caller ID authentication protocols exist which have been developed and are reasonably available for calls delivered over non-IP networks. We also find that a caller ID authentication protocol is "reasonably available" if the underlying equipment and software necessary to implement such protocol is available on the commercial market. We decline to adopt Alaska Communications' requirement that the underlying equipment and software be "widely available and affordable on

the commercial market," because the terms "widely" and "affordable," in the context of sophisticated businesses negotiating for specialized equipment and software, are too broad and indefinite to administer readily; and Alaska Communications does not provide enough further guidance on these terms to adopt them as part of a workable standard. We believe this approach is a workable and clear standard, and has support from the record. And as we have explained, we adopt the same standard for determining whether a caller ID authentication protocol is "effective" for purposes of our mandate on non-IP networks, ensuring a harmonious approach to our rules regarding non-IP caller ID authentication technology. Alaska Communications suggests that we adopt an additional requirement for determining whether a caller ID authentication protocol is "reasonably available." Specifically, Alaska Communications suggests that the "knowledge, training, and expertise necessary to operate the equipment and implement the standard [must be] sufficiently widespread among the small, rural, and other non-IP service providers" in receipt of an extension in order for the standard to be "reasonably available." We decline to adopt this requirement because doing so could create a perverse incentive for voice service providers to be willfully ignorant of newly developed protocols so as to prolong an extension. It also would require an unreasonably complicated inquiry into the knowledge and practices of numerous small voice service providers. We further find such a requirement to be unnecessary *ex ante* without a specific protocol and associated requirements in front of us.

69. As we explained in the context of the mandate on non-IP networks, we will continue to monitor industry progress towards the development of a non-IP caller ID authentication solution. If we find after providing notice and an opportunity for comment that a non-IP solution meets these criteria, we will both modify the non-IP implementation mandate and phase out the non-IP implementation extension to account for this new solution. Cooperative Telephone Company suggests that we grant a limited five-year extension of the June 30, 2021, deadline for implementing a caller ID authentication framework "for those service

providers currently using a TDM network that have less than 1,000 subscriber lines." Cooperative Telephone Company argues that such small and rural telephone companies have "scarce resources" which would not cover both the demands of their customers and new regulations for non-IP technology. We decline to do so given that such an extension would not be consistent with the timeframe that Congress established in the TRACED Act for the non-IP extension—which is to last until a non-IP solution becomes reasonably available—not for a fixed period of years. Alaska Communications suggests that we "grant a permanent exemption for the few non-SS7-connected switches remaining" because such switches are unique. We find adopting this proposal unnecessary at this time. In the absence of a developed solution, we are not yet in a position to determine whether any technical exceptions could be necessary and appropriate.

70. *Obligations of Voice Service Providers Receiving an Extension.* The TRACED Act provides that we should limit or terminate an extension of compliance if we determine in a future assessment that a voice service provider "is not making reasonable efforts to develop the call authentication protocol" for non-IP networks. To be consistent with our approach in mandating that voice service providers take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of their networks, we find that a voice service provider satisfies the "reasonable efforts" requirement under section 4(b)(5)(D) if it is able to provide the Commission, upon request, with documented proof that it is participating, either on its own, in concert with a vendor, or through a representative, as a member of a working group, industry standards group, consortium, or trade association that is working to develop a non-IP solution, or actively testing such a solution. We also conclude this requirement both promotes the IP transition and encourages the development of a non-IP authentication solution for the benefit of those networks that cannot be speedily or easily transitioned.

3. Reevaluating Granted Extensions

71. Section 4(b)(5)(F) of the TRACED Act requires us annually to reevaluate and

revise as necessary any granted extension, and "to issue a public notice with regard to whether such [extension] remains necessary, including why such [extension] remains necessary; and when the Commission expects to achieve the goal of full participation." As we proposed in our *First Caller ID Authentication Report and Order and FNPRM*, we direct the Bureau to reevaluate the extensions we have established annually, and to revise or extend them as necessary. We adopt this proposal because the Bureau is in the best position to undertake this fact-intensive and case-by-case evaluation, particularly in the context of evaluating extensions for undue hardship. Pursuant to the TRACED Act, we direct the Bureau to issue a Public Notice seeking comment to inform its annual review and consider the comments it receives before issuing a Public Notice of its decision as to whether to revise or extend an extension. The record reflects support, and no opposition, for this reevaluation process.

72. *Scope of Bureau's Authority.* We permit the Bureau to decrease, but not to expand, the scope of entities that are entitled to a class-based extension based on its assessment of burdens and barriers to implementation. Specifically, if the Bureau concludes in its review that a class-based extension should be extended beyond the original end date set by the Commission, it may choose to do so for all or some recipients of the extension, as it deems appropriate, based on its assessment and after providing notice and an opportunity for comment. As suggested by ACA Connects, we clarify that the Bureau may not, however, terminate an extension for some or all recipients prior to the extension's originally set or newly extended end date.

73. *Assessment of Burdens and Barriers.* The TRACED Act directs the Commission to assess burdens and barriers to implementation by December 30, 2020, and "as appropriate thereafter." We find it appropriate to reassess burdens and barriers to implementation by voice service providers that we granted an extension in conjunction with evaluating whether to maintain, modify, or terminate the extension. Accordingly, we direct the Bureau to assess burdens and barriers to implementation faced by those categories of voice service providers

subject to an extension when it reviews those extensions on an annual basis or on petition. Coordinating an assessment of burdens and barriers to implementation with our extension reevaluations will inform the Bureau's decision to extend or revise any granted extensions. It will also provide a basis for the Bureau to revise the scope of entities that are entitled to an extension. We find that aligning the periodic reassessment of burdens and barriers to implementation with any review of extensions is the best reading of the relevant statutory language. We read "appropriate" in this section to tie the timing of our future assessments to our annual extension reevaluations. We received no comments in the record to our proposal in this regard.

4. Robocall Mitigation Program

74. Section 4(b)(5)(C)(i) of the TRACED Act directs us to require any voice service provider that has been granted an extension to implement, during the time of the extension, "an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider." In the *First Caller ID Authentication Report and Order and FNPRM*, we sought comment on USTelecom's proposal to obligate voice service providers to file certifications describing their robocall mitigation programs in lieu of a prescriptive approach. In this Report and Order, we adopt this proposal and give voice service providers the flexibility to decide the specific contours of an effective robocall mitigation program that best suits the needs of their networks and customers. We additionally create a certification process and database to aid in enforcement efforts and prohibit intermediate providers and terminating voice service providers from accepting voice traffic from voice service providers not listed in the database. These steps will ensure that the only voice traffic to traverse voice networks in the U.S. is from those voice service providers that have either fully implemented STIR/SHAKEN on their entire networks or that have implemented a robocall mitigation program on those portions of their networks that are not STIR/SHAKEN-enabled.

75. *Providers Subject to the TRACED Act's Robocall Mitigation Program*

Requirement. Based on the statutory text, we read the requirement to implement a robocall mitigation program to apply to all voice service providers that receive an extension on the basis of undue hardship or material reliance on a non-IP network. The TRACED Act states that extensions for material reliance on a non-IP network are "[s]ubject to subparagraphs (C) through (F)," and paragraph (C)(i) sets forth the robocall mitigation program requirement. The record reflects support for this approach. Securus argues that we should not impose a robocall mitigation program requirement on voice service providers—even voice service providers granted an extension—whose networks uniquely pose "nearly zero" risk of originating high volumes of illegal robocalls. We decline to adopt this suggestion because the TRACED Act obligates us to require "any provider subject to such [extension to] implement an appropriate robocall mitigation program." Neustar recommends that we require "all voice service providers [to] utilize robocall mitigation solutions, regardless of whether they implement STIR/SHAKEN in their networks," and ZipDX argues that providers which have implemented STIR/SHAKEN should institute robocall mitigation programs for any calls they authenticate with C-level attestation. ZipDX also argues that we should require voice service providers to document and share with the Commission information on how they assign the A-, B-, or C-level attestations. We decline to adopt such a reporting requirement at this time, as we have no reason to believe the existing mechanisms for policing use of attestation levels within the STIR/SHAKEN framework are insufficient. We decline to adopt these suggestions. We agree with commenters that under the TRACED Act robocall mitigation "is intended to be an interim approach for addressing potential unlawful robocalls until the provider has implemented STIR/SHAKEN." Consistent with this view, in the case of voice service providers that have neither complied with the STIR/SHAKEN mandate by June 30, 2021, nor are subject to any extension, we expect such noncompliant voice service providers to implement robocall mitigation on the non-STIR/SHAKEN-enabled portions of their networks. Doing so does not free the provider from enforcement of its violation of our STIR/SHAKEN implementation mandate, but will protect

consumers by ensuring that no portion of the voice network is left without an implementation of either caller ID authentication or a robocall mitigation program. While USTelecom argues we can find authority under other provisions of the Act, we need not reach that issue. First, regardless of whether we could rely on an alternative source of authority, we find it appropriate to defer to Congress's recent, specific guidance on the subject. Moreover, while USTelecom argues that such a requirement "will provide benefits independent of call authentication solutions, including before and after full deployment of such solutions," we find such a requirement to be inappropriate at this juncture. We cannot yet know whether requiring voice service providers to expend additional resources on robocall mitigation even after STIR/SHAKEN implementation would be an efficient use of their resources, and we do not wish to place additional burdens on voice service providers already working to comply with the June 30, 2021, STIR/SHAKEN implementation deadline. We will revisit this conclusion if we determine that additional robocall mitigation efforts are necessary in addition to STIR/SHAKEN after the caller ID authentication technology is more widespread.

76. *Robocall Mitigation Program Requirements.* The TRACED Act directs us to require all voice service providers granted an extension—whether on the basis of undue hardship or material reliance on a non-IP network—to "implement an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the[ir] network[s]." As suggested by USTelecom, we require voice service providers subject to an extension to "take[] reasonable steps to avoid originating illegal robocall traffic." USTelecom outlines examples of such "reasonable steps," which could include "[a]nalyz[ing] high-volume voice network traffic to identify and monitor patterns consistent with robocall campaigns," "[a]nalyz[ing] traffic for patterns indicative of fraudulent calls—for example, identifying short duration calls with low completion rates," and "[t]ak[ing] reasonable steps to confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the general nature of the customer's

business." We decline to opine at this time on whether such practices meet our sufficiency standard, so as to promote experimentation with a wide variety of practices by voice service providers in their robocall mitigation programs. In a different proceeding, we propose requiring voice service providers to respond to traceback requests, mitigate illegal traffic when notified of such traffic, and take affirmative, effective measures to prevent new and renewing customers from using their networks to originate illegal calls; we also seek comment on whether we should prescribe specific steps. As our action in this proceeding is concerned with implementing section 4(b)(5)(C) of the TRACED Act, we do not preclude the possibility of requiring all voice service providers to take affirmative, effective measures to prevent the origination of unlawful calls—whether specific or not—pursuant to different legal authority, such as section 201(b) of the Communications Act of 1934, as amended. With one exception noted below, we find that a non-prescriptive approach to robocall mitigation requirements gives voice service providers "the flexibility to react to traffic trends they view on their own networks and react accordingly." This approach also allows voice service providers to innovate and "draw from the growing diversity and sophistication of anti-robocall tools and approaches available." In a separate proceeding, we proposed requiring voice service providers to take affirmative, effective measures to prevent new and renewing customers from using their networks to originate illegal calls, and seek comment on whether we should prescribe specific steps. As our analysis here is concerned with implementing section 4(b)(5)(C) of the TRACED Act, we do not preclude the possibility of requiring all voice service providers to take affirmative, effective measures to prevent the origination of unlawful calls—whether specific or not—pursuant to different legal authority, such as section 201(b) of the Act.

77. We require voice service providers subject to an extension to document and publicly certify how they are complying with these requirements. We find that such a requirement will encourage voice service providers to ensure that they are taking "reasonable steps." We have previously found that requiring self-evaluation is an effective means of

promoting compliance with our rules. In the rural call completion context, the Commission adopted a rule requiring covered providers to monitor the rural call completion performance of the calls they pass on to intermediate providers, and take action to address poor performance. We concluded that such a monitoring rule "will ensure better call completion to rural areas by covered providers, . . . reduce the necessity for enforcement action, and aid our enforcement efforts when needed." Such a requirement also enables us to evaluate a voice service provider's "reasonable steps" to determine whether they are sufficient. This public certification requirement will facilitate our ability to enforce a prohibition on intermediate providers and terminating voice service providers from accepting voice traffic from voice service providers with insufficient or ineffective robocall mitigation programs.

78. While we adopt a non-prescriptive approach to voice service providers' robocall mitigation programs, we find it necessary to articulate general standards, both to guide voice service providers in preparing their programs and to ensure that the statutory obligation to implement a robocall mitigation program is enforceable. We clarify that a robocall mitigation program is sufficient if it includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal robocalls. This is not to say that a voice service provider may not engage in practices, as part of its robocall mitigation program, that are experimental or cutting edge, and whose effectiveness is not yet proven. Rather, we encourage industry experimentation and only require that robocall mitigation programs include proven practices alongside experimental ones. In addition, for its mitigation program to be sufficient, the voice service provider must comply with the practices it describes. We will also consider a mitigation program insufficient if a provider knowingly or through negligence serves as the originator for unlawful robocall campaigns. We decline to adopt ZipDX's proposal that a robocall mitigation program merely be "effective" because ZipDX provides no elaboration of how to define the term, and we think the more detailed requirement we adopt will be both clearer and more successful than a non-specific "effective" standard. At the same time, we agree with

Verizon that "different types of network providers should have different types of robocall mitigation programs," and we welcome voice service providers adopting approaches that are innovative, varied, and adapted to their networks.

79. The record also convinces us that participation in industry traceback efforts is of utmost importance in the absence of STIR/SHAKEN implementation. To that end, we require voice service providers, as part of their robocall mitigation programs, to commit to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls. We underscore that this requirement does not supersede any existing legal processes. We also encourage law enforcement to make traceback requests through the industry traceback consortium. We find that this baseline requirement to participate in traceback efforts is a necessary aspect of any attempt to mitigate illegal robocalls, as it permits voice service providers and enforcement agencies to identify illegal robocallers and prevent them from further abusing the voice network. Without a means to identify and bring enforcement actions against the sources of illegal robocalls, such bad actors will continue their operations unchecked and emboldened. We underscore that this is a necessary, but not sufficient, component of a voice service provider's robocall mitigation program which, as we have explained, must include other steps to ensure that a provider is not the source of illegal robocalls.

80. We decline at this time to impose other more prescriptive requirements for robocall mitigation programs, such as mandating an analytics-based robocall mitigation program, as proposed by Transaction Network Services, or know-your-customer policies, as suggested by Consumer Groups. While we acknowledge that such practices and policies may be effective aspects of a robocall mitigation program—and we encourage voice service providers to incorporate them into their own robocall mitigation programs—we decline specifically to mandate them, as we agree with commenters that argue that there is no one-size-fits-all robocall mitigation solution that accounts for the variety and scope of voice service provider networks.

For example, a small voice service provider with few subscribers may not have a need to implement comprehensive analytics given its small size. Similarly, a voice service provider with limited means may choose a solution suited to its budget and business model. We also decline Neustar's suggestion that we "ensure that providers implement robocall mitigation solutions for both originating and terminating calls." The TRACED Act's mandate plainly requires only robocall mitigation programs that "prevent unlawful robocalls from *originating* on the network of the provider."

81. *Deficient Robocall Mitigation Programs*. If we find that our non-prescriptive approach to robocall mitigation is not satisfactorily stemming the origination of illegal robocalls, we agree with NTCA and Verizon that we should be ready to impose more prescriptive obligations on any voice service provider whose robocall mitigation program has failed to prevent high volumes of illegal robocalls. We thus direct the Enforcement Bureau to prescribe more specific robocall mitigation obligations for any voice service provider it finds has implemented a deficient robocall mitigation program. Such robocall mitigation obligations would be chosen as appropriate to resolve the specific voice service provider's prior shortcomings. In such instances, the Enforcement Bureau will release an order explaining why a particular mitigation program is deficient and, among other things, prescribe the new obligations needed to rectify those deficiencies, including any milestones or deadlines. We find that action by the Enforcement Bureau is appropriate in responding to issues on a case-by-case basis. As part of the penalties it may impose, the Enforcement Bureau may de-list a voice service provider from the robocall mitigation database we establish. If we find that our non-prescriptive approach to robocall mitigation programs is falling short on a widespread basis, we will not hesitate to revisit the obligations we impose through rulemaking at the Commission level.

82. *Voice Service Provider Certification and Database.* To promote transparency and effective robocall mitigation, we require all voice service providers—not only those granted an extension—to file certifications with the Commission regarding their efforts to stem the

origination of illegal robocalls on their networks. Specifically, as proposed by USTelecom, and with the support of all parties that commented on the issue in the record, we require all voice service providers to certify that their traffic is either "signed with STIR/SHAKEN or . . . subject to a robocall mitigation program" that includes "tak[ing] reasonable steps to avoid originating illegal robocall traffic," and committing to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls. For those voice service providers that certify that some or all of their traffic is "subject to a robocall mitigation program," we require such voice service providers to detail in their certifications the specific "reasonable steps" that they have taken "to avoid originating illegal robocall traffic." This requirement will promote transparency and accountability in light of our non-prescriptive approach to the robocall mitigation program requirements. While only voice service providers with an extension will be obligated to implement a robocall mitigation program, we impose the certification requirement on all voice service providers because doing so will help us and others to hold all voice service providers accountable for the voice traffic they originate, and give us and others a snapshot of the progress of STIR/SHAKEN implementation and the variety of robocall mitigation practices adopted by voice service providers.

83. Voice service providers must file certifications via a portal on the Commission's website that we will establish for this purpose. We will also establish a publicly accessible database in which we will list such certifications. Establishing a database will aid in monitoring compliance with our robocall mitigation requirement and facilitate enforcement action should such action be necessary. We direct the Bureau to establish this portal and database, provide appropriate filing instructions and training materials, and release a Public Notice when voice service providers may begin filing certifications. We direct the Bureau to release this Public Notice no earlier than March 30, 2021, and to establish a deadline for the filing of certifications no earlier than June 30, 2021. Verizon argues that we "need not wait until 2021 to establish a

registry with a certification requirement and issue rules imposing robocall mitigation obligations on all traffic originated by any service provider." We disagree and instead find it appropriate to harmonize this requirement—which is tied by statute to receiving an extension from the STIR/SHAKEN implementation mandate—to the date the STIR/SHAKEN mandate goes into effect. However, we agree with Verizon that "consumers should get the benefits of the registration framework and the robocall mitigation rules this year," and encourage providers to take efforts toward robocall mitigation as soon as possible. We also direct the Bureau to issue guidance and a protective order regarding the treatment of any confidential and highly confidential information included in certifications. We do so to protect voice service providers that are worried that public disclosure of their robocall mitigation programs may give bad actors the information they need to undermine their programs, or necessitate disclosure of competitively sensitive information. If we find that a certification is deficient in some way, such as if the certification describes a robocall mitigation program that is ineffective, or if we find that a provider nonetheless knowingly or negligently originates illegal robocall campaigns, we may take enforcement action as appropriate. Enforcement actions may include, among others, removing a defective certification from the database after providing notice to the voice service provider and an opportunity to cure the filing, or requiring the voice service provider to submit to more specific robocall mitigation requirements, and/or imposition of a forfeiture.

84. We also require voice service providers filing certifications to provide the following identification information in the portal on the Commission's website:

(1) the voice service provider's business name(s) and primary address;

(2) other business names in use by the voice service provider;

(3) all business names previously used by the voice service provider;

(4) whether a voice service provider is a foreign voice service provider; and

(5) the name, title, department, business address, telephone number, and email address of a central point of contact within the company responsible for addressing robocall-

mitigation-related issues.

85. This information will be made publicly available in the database, and reporting such information presents a minimal burden on voice service providers. We find that requiring a voice service provider to report contact information for the person responsible for addressing robocall-mitigation-related issues will facilitate inter-provider cooperation and enforcement actions should issues arise. We also require voice service providers to submit to the Commission via the appropriate portal any necessary updates to the information they filed in the certification process within 10 business days. This requirement will ensure that we and all voice service providers have up-to-date data without overburdening voice service providers with unnecessary filings.

86. *Obligations on Intermediate Providers and Terminating Voice Service Providers.* As suggested by multiple commenters, we prohibit intermediate providers and terminating voice service providers from accepting voice traffic directly from any voice service provider that does not appear in the database, including a foreign voice service provider that uses NANP resources that pertain to the United States to send voice traffic to residential or business subscribers in the United States. ZipDX suggests that we prohibit intermediate providers and terminating voice service providers from accepting voice traffic from foreign voice service providers using U.S. numbers unless the foreign voice service provider is listed in the robocall mitigation database and the domestic provider can provide an A-level attestation for the call. We decline to take this approach at this time as industry has not yet coalesced around an approach to A-level attestations for foreign-originated calls. Effective 90 days after the deadline for robocall mitigation program certifications set forth in the Bureau Public Notice establishing the robocall mitigation database and portal, intermediate providers and terminating voice service providers are subject to this prohibition. The record reflects support for this requirement.

87. We agree with Verizon that, "by prohibiting downstream service providers from accepting traffic from providers that are not in [the database], the Commission can deny a service

provider access to the regulated U.S. voice network if it determines that the service provider's STIR/SHAKEN or robocall mitigation practices are inadequate." In this way, we can police the voice traffic that voice service providers originate by removing or restoring a voice service provider's listing on the database, after providing notice of any certification defects and providing an opportunity to cure. Furthermore, as voice service providers monitor the database to ensure they remain compliant with our rules, they must necessarily review the listings of voice service providers with which they interconnect to ensure that such certifications are sufficient. In so doing, industry continually reviews itself to ensure compliance with our rules, amplifying the effectiveness of our own review. This rule will further encourage all voice service providers to implement meaningful and effective robocall mitigation programs on their networks during the period of extension from the STIR/SHAKEN mandate. In turn, this rule will help prevent illegal robocall traffic from reaching terminating voice service providers and their subscribers. To ease compliance with this obligation, we will import all listings from the Intermediate Provider Registry into the Robocall Mitigation Database on a rolling basis so that all registered intermediate providers are represented therein. Because intermediate providers that do not originate any traffic are not subject to our certification requirements, they would not otherwise be listed in the database. By affirmatively adding such providers we give intermediate and terminating voice service providers confidence that any provider not listed in the Robocall Mitigation Database is out of compliance with our rules, rather than leaving the potential for uncertainty about whether a provider is noncompliant or simply was not required to be included in the database because it does not originate traffic. A provider that serves as both an intermediate provider and originating voice service provider must file a certification with respect to the traffic for which it serves as an originating voice service provider, even if its listing has been imported from the Intermediate Provider Registry.

88. NTCA and ACA argue that we should require intermediate providers and terminating voice service providers to give notice to an originating voice service provider whose

traffic they will block because it is not listed in the robocall mitigation database. NTCA argues that this will "enable legitimate providers to cure honest mistakes on their part or 'glitches' in the database." We decline to adopt this suggestion as we find that the framework we adopt provides adequate notice to voice service providers of the need to file sufficient certifications, including a 90-day period between the deadline for certifications and the prohibition on intermediate and terminating voice service providers accepting traffic from originating voice service providers not in the database. Second, adopting this suggestion would place potentially costly obligations on *compliant* intermediate providers and terminating voice service providers to provide adequate notice to *noncompliant* originating voice service providers. Such compliant providers may be unable to provide notice for lack of having or being able to obtain a noncompliant provider's contact information—opening themselves up to potential enforcement action for lack of compliance. Lastly, we will give notice and an opportunity to cure to voice service providers whose certifications are deficient before we take enforcement action such as de-listing the provider from the database.

89. We decline to adopt to USTelecom's proposal that we require intermediate providers to file a certification to their compliance with this rule. We see no clear need to impose a burdensome belt-and-suspenders paperwork requirement on providers that are already subject to this obligation by rule. We similarly decline ZipDX's proposal that intermediate providers must "[i]mplement[] a Robocall Mitigation Program applicable to calls [they do] not authenticate." This includes intermediate providers acting as domestic gateway providers for foreign-originated calls. Pursuant to the TRACED Act, robocall mitigation is meant to stem the *origination* of illegal robocalls, and ZipDX does not explain specifically how an intermediate provider could itself prevent the origination of illegal robocalls. We find the rule we establish—whereby intermediate providers are prohibited from accepting traffic from an originating voice service provider that has not certified to a robocall mitigation program—best leverages the role of intermediate providers to combat illegal robocalls within our greater robocall mitigation

scheme.

90. *Foreign Voice Service Providers.* In the *First Caller ID Authentication Report and Order and FNPRM*, we sought comment on mechanisms to combat robocalls originating abroad. The record contains several comments expressing support for combating robocalls originating abroad by requiring foreign voice service providers that wish to appear in the database to follow the same requirements as domestic voice service providers, and we do so in this document. Thus, foreign voice service providers that use NANP numbers that pertain to the United States to send voice traffic to residential and business subscribers in the United States must follow the same certification requirements as domestic voice service providers in order to be listed in the database. Because we prohibit domestic intermediate providers and terminating voice service providers from accepting traffic from foreign voice service providers that use NANP numbers that pertain to the United States and are not listed in the database, we create a strong incentive for such foreign voice service providers to file certifications. We note for the sake of clarity, however, that we do not *require* foreign voice service providers to file a certification; though intermediate providers and terminating voice service providers are prohibited from accepting traffic from foreign voice service providers who do not appear in the robocall mitigation database.

91. We find that this result will encourage foreign service providers to choose to institute robocall mitigation programs and file certifications to be listed in the database and thus have their traffic be accepted by domestic intermediate and terminating voice service providers. The measures we adopt in this document will also enable foreign voice service providers to continue using U.S. telephone numbers to send voice traffic to U.S. subscribers under the same certification procedures that will apply to U.S. voice service providers and thereby help prevent the fraudulent exploitation of NANP resources and reduce the volume of illegal voice traffic entering the United States. Ensuring that foreign voice service providers using U.S. telephone numbers comply with the certification requirements prior to being listed in the database is

especially important in light of the prevalence of foreign-originated illegal robocalls aimed at U.S. consumers and the difficulty in eliminating such calls.

92. We find persuasive the argument by ZipDX that the definition in the initially circulated and publicly released draft Order, which defined "foreign voice service provider" as "any entity that is authorized within a foreign country to provide international voice service," was unduly narrow and excluded non-U.S. providers that do not possess any authorization to provide service from being able to file certifications and be listed in the database. In response, we revise our rules to establish that an entity is a "foreign voice service provider" if such entity has the ability to originate voice service that terminates in a point outside a foreign country or terminate voice service that originates from points outside that foreign country. Specifically, we define "foreign voice service provider" to mean "any entity providing voice service outside the United States that has the ability to originate voice service that terminates in a point outside that foreign country or terminate voice service that originates from points outside that foreign country." We find that this approach captures voice traffic originating from a broader range of foreign voice service providers than the one that initially appeared in the draft.

93. Under the rules we adopt, foreign voice service providers that use U.S. telephone numbers to send voice traffic to U.S. subscribers must file the same certification as U.S. voice service providers in order to be listed in the database. Specifically, to be listed in the database, these providers must certify either that they have implemented STIR/SHAKEN or comply with the robocall mitigation program requirements outlined above by "tak[ing] reasonable steps to avoid originating illegal robocall traffic" and committing to cooperating with the Commission, U.S. law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls. If we find that a voice service provider's certification is deficient or the provider fails to meet the standards of its certification, we will pursue enforcement including de-listing the provider from the database. We further note that, as discussed above, we require voice service providers—including foreign

voice service providers that wish to be listed in the database—to submit to the Commission any necessary updates regarding any of the information they filed in the certification process within 10 business days.

94. Although USTelecom, following circulation and public release of a draft of this Order, has changed its position and now suggests seeking further comment on this approach, we nevertheless take action in this document given the crucial and urgent importance of protecting Americans from illegal and fraudulent foreign-originated robocalls. USTelecom, along with CTIA, suggest that our action in this document could result in unforeseen technical issues, or the blocking of legitimate calls. ZipDX disagrees with this suggestion, arguing that any impact that could arise would be minimal and could be promptly resolved. As our rules related to foreign-originated voice traffic that we take in this document will not begin to affect such voice traffic until June 2021, we are optimistic that voice service providers will have time to resolve any identified issues before the deadline. Should voice service providers identify concrete evidence of technical problems or likely blocking of legitimate calls, we encourage them to provide us such information so that we can consider whether to make any modifications to this rule.

5. Alternative Methodologies During an Extension

95. The TRACED Act directs us to "identify, in consultation with small providers of voice service, and those in rural areas, alternative effective methodologies to protect consumers from unauthenticated calls during any" extension from compliance with our STIR/SHAKEN implementation mandate. The TRACED Act does not specify that voice service providers may substitute such methods for the robocall mitigation program that it requires, and we read the TRACED Act as merely calling for us to identify additional options for voice service providers subject to extension that wish to better serve their customers and the public by going above and beyond their legal obligations. Given that caller ID authentication frameworks are not yet ubiquitous—and thus most calls that transit U.S. voice networks are unauthenticated—we understand Congress's concern in this provision to be about protecting consumers from

unauthenticated, illegally spoofed robocalls. We therefore interpret a methodology to be "effective" if it is likely to substantially reduce the volume of illegal robocalls reaching subscribers. In our *Third Call Blocking Report and Order*, we adopted a safe harbor in our call blocking rules for voice service providers that use reasonable analytics that include caller ID authentication information to inform their call blocking services. We find that these types of call blocking services would likely reduce the volume of unauthenticated illegal robocalls reaching subscribers, and thus include them in this definition. We find that this definition tracks the overall purpose of the TRACED Act which is "to reduce illegal and unwanted robocalls" through various mechanisms. We sought comment in the *First Caller ID Authentication Report and Order and FNPRM* from small and rural voice service providers on such alternative effective methodologies. The record we received in response demonstrates that such alternative methodologies either already exist or are in development. To fulfill this obligation, we identify the following alternative effective methodologies recommended by small and rural voice service providers, as well as other commenters:

- Innovative Systems reports that its landline call blocking service is "fully developed and currently installed at 207 landline providers" and, in the last nine years, "has challenged over 19 million suspected spam calls and blocked another 12 million calls that were from phone numbers off the FCC's weekly robocall and telemarketing consumer complaint data reports." It states that "greater consumer protection can be achieved by having this alternative methodology installed on all landlines using an opt-out strategy at no cost, versus a purchase to opt-in by the customer."
- Neustar reports that its robocall mitigation service "helps voice service providers block calls from illegal robocallers and helps end users identify robocalls . . . . [b]y combining authoritative data . . . with behavior insights."
- Transaction Network Services reports that "[c]all analytics have proven successful in identifying a large number of the problematic calls being transmitted

today. . . . Reasonable call analytics are widely available from multiple vendors, many of which offer low-investment services that can be deployed in smaller networks at a reasonable cost."

96. Additionally, the recent call blocking report released by the Consumer and Governmental Affairs Bureau identified various available effective methodologies for protecting subscribers from illegal calls, a sample of which is reproduced below:

Business name	**Blocking/labeling services offered**	**Estimate on number of calls blocked or labeled**	**Default, opt-in, or opt-out**
AT&T—Wireless	Network-level blocking Call Protect or Call Protect Basic, free Call Protect Plus	Call Protect and Call Protect Plus, since 2016, blocked fraudulent calls or labeled suspicious calls; nearly 1.3 billion suspected fraud and over 3 billion other calls blocked or labeled.	Network-level blocking is default Call Protect is opt-out, since 2019 Call Protect Plus is opt-in
AT&T—VoIP	Network-level blocking Digital Phone Call Protect, free	Blocked over 46 million and spam warnings for 36 million.	Network-level blocking is default Digital Phone Call Protect is opt-in
Call Control (third-party analytics	Software-based call blocking	Blocked over one billion calls.	N/A

company)			
Comcast—Wireline	Network-level blocking Anonymous Call Rejection, Selective Call Rejection, free Customers can sign up for Nomorobo blocking service, free	Over 158 million calls blocked in Dec. 2019. Anonymous Call Rejection blocked nearly 37 million calls in Dec. 2019. Selective Call Rejection blocked over five million calls in Dec. 2019.	Network-level blocking is default Anonymous Call Rejection is opt-in, but will be offered opt-out; Selective Call Rejection is opt-in Nomorobo is opt-in
Cox	Edge Blocking, free Anonymous Call Rejection, Selective Call Rejection, free Customers can sign up for Nomorobo blocking service, free.	14.6% of calls are blocked through one of these tools; Edge Blocking is 65% of the blocked calls and Anonymous Call Rejection is 29%t.	Edge Blocking is opt-out Anonymous Call Rejection and Selective Call Rejection are opt-in
First Orion (third-party analytics company)	Scam ID and Scam Block	Since 2017, identified over 22 billion scam calls.	N/A

Hiya (third-party analytics company)	Call blocking	Since 2016, blocked or labeled nearly 1.3 billion suspected fraud calls and over 3 billion other suspect calls.	N/A
Nomorobo (third-party analytics company)	Call blocking	As of April 30, 2020, blocked over 1.6 billion robocalls.	N/A
T-Mobile	Scam ID, free Scam Block, free Name ID, free for some plans	Since 2017, identified over 21 billion scam calls and blocked over 5 billion of those calls.	Scam ID is opt-out for post-paid customers Scam Block is opt-in
Verizon—Wireless	Network-level blocking Call Filter, free	Since 2017, blocked hundreds of millions of calls.	Network-level blocking is default Call Filter is opt-out
Verizon—Wireline	Network-level blocking Spam Alert, free VoIP customers can	Since 2017, blocked hundreds of millions of calls.	Network-level blocking is default Spam Alert is default Nomorobo is opt-in

	sign up for Nomorobo blocking service, free		

6. Legal Authority

97. The TRACED Act expressly directs us to grant extensions for compliance with the STIR/SHAKEN implementation mandate, require any voice service provider subject to such an extension to implement a robocall mitigation program to prevent unlawful robocalls from originating on its network, and place unique obligations on providers that receive an extension due to material reliance on non-IP network technology. The TRACED Act thus provides a clear source of authority for the rules we adopt in this document.

98. We conclude that section 251(e) of the Act provides additional, independent authority to adopt the extensions and associated requirements. That section gives us exclusive jurisdiction over numbering policy and enables us to act flexibly and expeditiously with regard to important numbering matters. When bad actors unlawfully falsify or spoof the caller ID that appears on a subscriber's phone, they are using numbering resources to advance an illegal scheme. The extensions and associated requirements will help to prevent the fraudulent exploitation of NANP resources by permitting those providers and their subscribers to identify when caller ID information has been spoofed.

99. We conclude that section 251(e) gives us authority to prohibit intermediate providers and voice service providers from accepting traffic from both domestic and foreign voice service providers that do not appear in our newly established database. We emphasize that the rule we adopt in this document does not constitute the exercise of jurisdiction over foreign voice service providers. We acknowledge that this rule will have an indirect effect on foreign voice service providers by incentivizing them to certify to be listed in the database. An indirect effect on foreign voice service providers, however, "does not militate against the validity of rules

that only operate directly on voice service providers within the United States." As we concluded in the *First Caller ID Authentication Report and Order*, our exclusive jurisdiction over numbering policy provides authority to take action to prevent the fraudulent abuse of NANP resources. Illegally spoofed calls exploit numbering resources whenever they transit any portion of the voice network—including the networks of intermediate providers. Our action preventing such calls from entering an intermediate provider's or terminating voice service provider's network is designed to protect consumers from illegally spoofed calls, even while STIR/SHAKEN is not yet ubiquitous. Verizon agrees that section 251(e) gives us ample authority to ensure foreign VoIP providers "submit to the proposed registration and certification regime by prohibiting regulated U.S. carriers from accepting their traffic if they do not."

100. We additionally find authority in the Truth in Caller ID Act. We find that the rules we adopt in this document are necessary to enable voice service providers to help prevent these unlawful acts and to protect voice service subscribers from scammers and bad actors, and that section 227(e) provides additional independent authority for the rules we adopt in this document.

D. Voluntary STIR/SHAKEN Implementation Exemption

101. While the TRACED Act directs us to require each voice service provider to implement STIR/SHAKEN in its IP network, section 4(b)(2) of the TRACED Act frees a voice service provider from this requirement if we determine, by December 30, 2020, that "such provider of voice service": (A) "in [IP] networks"—(i) "has adopted the STIR/SHAKEN authentication framework for calls on the [IP] networks of the provider of voice service; (ii) has agreed voluntarily to participate with other providers of voice service in the STIR/SHAKEN authentication framework; (iii) has begun to implement the STIR/SHAKEN authentication framework; and (iv) will be capable of fully implementing the STIR/SHAKEN authentication framework" not later than June 30, 2021; and (B) "in non-[IP] networks"—(i) "has taken reasonable measures to implement an effective call authentication framework; and (ii) will be

capable of fully implementing an effective call authentication framework" not later than June 30, 2021.

102. Below, we read section 4(b)(2) of the TRACED Act as creating two exemptions: one for IP calls and one for non-IP calls. To ensure that the exemption only applies where warranted and to provide parties with adequate guidance, we expand on each of the prongs that a voice service provider must meet to obtain an exemption, and adopt rules accordingly. We find that the best way to implement the TRACED Act's exemption provision in a timely manner is via a certification process and thus adopt rules requiring that a voice service provider that wishes to receive an exemption submit a certification that it meets the criteria for the exemptions that we have established pursuant to section 4(b)(2)(A), section 4(b)(2)(B), or both. To guard against the risk of gaps and improper claims of the exemption, we require voice service providers that receive an exemption to file a second certification after June 30, 2021, stating whether they, in fact, achieved the implementation goal to which they previously committed in their initial certification. Last, we find that the TRACED Act's exemption provision does not extend to intermediate providers. We adopt these rules pursuant to the authority expressly granted us by section 4(b)(2) of the TRACED Act.

1. Relationship of IP Networks and Non-IP Networks Provisions

103. As proposed in the *Further Notice of Proposed Rulemaking*, we read section 4(b)(2) of the TRACED Act as creating two exemptions: one for IP calls and one for non-IP calls. Thus, a voice service provider may seek the exemption for its "IP networks" if it meets all four criteria for all calls it originates or terminates in SIP, and a voice service provider may seek the exemption for its "non-IP networks" if it meets both the criteria for all non-SIP calls it originates or terminates. This approach is consistent with the views of the commenters that touched upon this issue in the record.

104. We find that this reading best implements Congress's policy and is consistent with principles of statutory construction when considering the statute as a whole. As AT&T

observes, the structure of the TRACED Act "recognizes that implementation of a caller ID authentication framework will differ for IP networks and non-IP networks." Given the presence of the word "and" between the IP and non-IP networks criteria, we recognize that the exemption could potentially be read as applying only if the voice service provider meets both the IP and non-IP networks criteria. Yet such a reading would render the exemption an empty set or nearly so because of the absence of an effective solution for non-IP caller ID authentication at present, such that few, if any, voice service providers will be able to claim that they will be capable of "fully implementing" an effective non-IP caller ID authentication framework by June 30, 2021. Our reading cabins the nullity risk more narrowly, thus better effectuating Congress's goal of creating a meaningful exemption.

105. Our approach also further encourages prompt deployment of STIR/SHAKEN. We understand the statutory exemption to both encourage and reward early progress in deployment. Therefore, by giving voice service providers a path to exemption solely for their IP networks—the only types of networks on which STIR/SHAKEN can effectively operate—our approach will effectuate Congress's intent to encourage faster progress in STIR/SHAKEN deployment. And by separating IP and non-IP calls in this way, we align our exemption process with the call-by-call vision of a caller ID authentication implementation mandate that subjects different parts of a voice service provider's network to different requirements.

2. Threshold for IP Networks Exemption

106. To ensure that the exemption only applies where warranted and to provide parties with adequate guidance, we expand on each of the four substantive prongs laid out in the TRACED Act that a voice service provider must meet to obtain an exemption.

107. *Prong (i)—Adoption of STIR/SHAKEN.* In the *Further Notice of Proposed Rulemaking*, we proposed to interpret the phrase "has adopted the STIR/SHAKEN authentication framework for calls on the [IP] networks of the provider of voice service" in prong (A)(i) to mean that the voice service provider has publicly committed, via a certification, to complete

implementation of STIR/SHAKEN by June 30, 2021. In light of the comments in the record, we modify this proposal to require that the voice service provider has completed the network preparations necessary to deploy the STIR/SHAKEN protocols on its network, including, but not limited to, by participating in test beds and lab testing, or completing commensurate network adjustments to enable the authentication and validation of calls on its network consistent with the STIR/SHAKEN framework.

108. We agree with commenters that focusing on network preparations will provide significant concrete evidence that a voice service provider is taking the necessary steps in its STIR/SHAKEN implementation, and will thus offer confirmation that a provider has adopted the STIR/SHAKEN authentication framework. We further agree with AT&T that our original certification-based proposal would not provide specific measurable criteria by which to assess a provider's progress. Simply issuing a commitment will not do as much to ensure that voice service providers are actually doing so as will an obligation to undertake the network preparations necessary to operationalize the STIR/SHAKEN protocols on their networks. Taking the necessary first steps to participate in STIR/SHAKEN more affirmatively demonstrates a voice service provider's commitment and preparedness to implement an effective caller ID authentication framework than a general declaration of intent that may or may not be accompanied by concrete steps. We disagree with T-Mobile's unsupported contention that our previous proposal would be preferable. While a public commitment to complete implementation of STIR/SHAKEN by June 30, 2021 would be a welcome initial step, we conclude that the better approach is to require voice service providers to undertake the preparations necessary to implement this framework, rather than merely issuing a pledge to do so.

109. *Prong (ii)—Participation with Other Providers.* In the *Further Notice of Proposed Rulemaking*, we proposed to read the phrase "has agreed voluntarily to participate with other providers of voice service in the STIR/SHAKEN authentication framework" in prong (A)(ii) to require that the voice service provider has written, signed agreements with at least two

other voice service providers to exchange calls with authenticated caller ID information. After reviewing the record, we revise this proposal to require that the voice service provider has demonstrated its voluntary agreement to participate with other voice service providers in the STIR/SHAKEN framework by completing formal registration (including payment) and testing with the Policy Administrator.

110. We agree with commenters that such an action would signal both a public and financial commitment to working with other voice service providers sufficient to confirm a provider's coordination efforts. Registering with the Policy Administrator is a necessary predicate to participation with other voice service providers in the STIR/SHAKEN framework, and was formulated by the industry to allow the exchange of authenticated traffic without requiring dedicated agreements between voice service providers. Completing formal registration and testing with the Policy Administrator thus signals both a voice service provider's technical readiness and willingness to participate with other providers in the STIR/SHAKEN framework. We further agree with AT&T, CTIA, and CCA that our initial proposal ignores certain market realities by assuming that every provider of voice services will require multiple agreements to exchange traffic destined to every point on the PSTN. Given that some voice service providers may not require two or more interconnection arrangements, let alone multiple agreements with other providers, to exchange their IP-based traffic, imposing a two-agreement requirement to demonstrate voluntary participation in the STIR/SHAKEN framework would be arbitrary and might even inject artificial inefficiencies into such arrangements. Our revised interpretation of prong (A)(ii) more closely aligns with the language and intended purpose of the statute, and better encourages STIR/SHAKEN implementation without introducing potential inefficiencies. Exchanging traffic using certificates assigned through the governance system is exactly the way STIR/SHAKEN is designed to work. Encouraging voice service providers to complete formal registration and testing with the Policy Administrator is thus the most appropriate and reasonable interpretation of the requirement in prong (A)(ii).

111. *Prong (iii)—Begun to Implement.* As proposed in the *Further Notice of Proposed Rulemaking*, we implement the phrase "has begun to implement the STIR/SHAKEN authentication framework" in prong (A)(iii) by requiring that the voice service provider has completed the necessary network upgrades to at least one network element (e.g., a single switch or session border controller) to enable the authentication and verification of caller ID information consistent with the STIR/SHAKEN standards. This interpretation requires a voice service provider to make meaningful progress on implementation by the time of certification, while taking into account that voice service providers will have limited time between adoption of this Order and the December 30, 2020 deadline for exemption determinations. While CCA argues that our approach is unachievable and overly prescriptive, we disagree. To the contrary, our approach accounts for the abbreviated timeframe by giving voice service providers the flexibility to choose to complete upgrades on the network element which they can upgrade most efficiently.

112. In this case, we find USTelecom's suggestion that we require voice service providers to establish the capability to authenticate originated traffic and/or validate such traffic terminating on their networks to be excessively vague, and it is unclear how little or how much voice service providers would be required to do under such a rule. Depending on the voice service provider, simply "establishing" the capability to authenticate originated traffic and/or validate such traffic terminating on their networks could consist of fully implementing this capability or merely attaining this capability without actually deploying it in one's network. To the extent that USTelecom—which does not provide a rationale for its proposal—is concerned that the standard we adopt will be too easily met, we are confident that the opportunity to verify implementation of an effective authentication framework will help identify any voice service providers that fail to meet their STIR/SHAKEN implementation commitments.

113. *Prong (iv)—Capable of Fully Implementing.* Last, and as proposed in the *Further Notice of Proposed Rulemaking*, we implement the obligation to "be capable of fully implementing the STIR/SHAKEN authentication framework" not later than June 30, 2021, in

prong (A)(iv) so as to require that the voice service provider reasonably foresees that it will have completed all necessary network upgrades to its network infrastructure to be able to authenticate and verify caller ID information for all SIP calls exchanged with STIR/SHAKEN-enabled partners by June 30, 2021. After considering the arguments in the record, we agree with T-Mobile that our proposal is preferable to USTelecom's narrower alternative of requiring a certification that all consumer VoIP and VoLTE traffic originating or terminating on a voice service provider's network either is or will be capable of authentication and validation by June 30, 2021. This requirement falls short of our implementation mandate, which requires that *all* calls be subject to caller ID authentication and verification—not just consumer VoIP and VoLTE traffic—except for those subject to the narrow and time-limited extensions we adopt in this document. To grant an exemption for voice service providers that will be capable of anything short of full compliance would indefinitely leave out calls the TRACED Act and our rules thereunder require to be subject to caller ID authentication. Such an approach also is inconsistent with the statute, which requires "full[] implementation[]" by June 30, 2021, so it is appropriate for us to demand that a provider reasonably foresee that it will meet that standard, rather than set a bar that is more easily cleared at the twelve-month mark but that heightens the risk of a voice service provider ultimately falling short just six months later. While we understand AT&T's point that voice service providers with more complex, diverse networks will necessarily have more complicated and costly STIR/SHAKEN implementation requirements, we do not think that our proposal is "overly rigid" or "ambiguous." Nor do we agree with CCA that it is "overly prescriptive." Rather, we institute a clear requirement that voice service providers "reasonably foresee" that they will be able to meet the standard Congress established by the deadline that Congress established. This interpretation gives as much latitude to voice service providers as possible to achieve the desired benchmarks while still requiring some basis for the claim that a provider is "capable of fully implementing the STIR/SHAKEN authentication framework."

3. Threshold for Non-IP Networks Exemption

114. Under the TRACED Act, a voice service provider is excused from the requirement to take reasonable measures to implement an effective caller ID authentication framework in the non-IP portions of its network if the Commission finds that it: (1) has taken reasonable measures to implement an effective caller ID authentication framework in the non-IP portions of its network; and (2) will be capable of fully implementing an effective caller ID authentication framework in the non-IP portions of its network not later than June 30, 2021. While we anticipate that in the non-IP context few if any voice service providers will seek to take advantage of this exemption because of the difficulties in "fully implementing an effective caller ID authentication framework" by June 30, 2021, we nevertheless adopt standards for determining whether a voice service provider has met both requirements necessary to receive an exemption under section 4(b)(2)(B) of the TRACED Act for the non-IP portions of its network, as required by the TRACED Act.

115. In the *Further Notice of Proposed Rulemaking*, we sought comment on section 4(b)(2)(B) and whether there was an "acceptable interpretation of the 'fully implementing' prong that would make it more achievable for voice service providers to qualify for the exemption." We further sought comment on what constitutes an "effective" call authentication framework and "reasonable measures" for purposes of this section. We now find that a voice service provider satisfies the first prong—requiring reasonable measures to implement an effective caller ID authentication framework—if it can certify that it is working to develop a non-IP authentication solution. Because the statutory language is similar to that used to establish the non-IP mandate, we find it appropriate to harmonize our interpretation of these two provisions. Section 4(b)(1)(B) of the TRACED Act requires a voice service provider "to take reasonable measures to implement an effective call authentication framework" in the non-IP portions of its networks, while section 4(b)(2)(B)(i) requires that a voice service provider "has taken reasonable measures to implement an effective call authentication framework" in the non-IP portions of its network.

While we recognize the difference in tenses between the two provisions—one refers to taking reasonable measures, while the other states that such measures must have already been taken—the remaining language is identical. Thus, we find that the two provisions are similar enough to implement the same standard in order to quantify what constitutes "reasonable measures" in both instances. Further, adopting a uniform approach allows us to avoid creating unnecessarily burdensome overlapping, but distinct, requirements. While we harmonize these provisions, we do not include the first method of compliance with our non-IP mandate, which a provider satisfies by completely upgrading its non-IP networks to IP and implementing the STIR/SHAKEN authentication framework. A provider that has completely upgraded its non-IP networks to IP would be subject to the exemption for IP networks, rather than the exemption for non-IP networks, and would be required to satisfy the requirements laid out for that exemption.

116. AT&T supports a proposal to require providers to participate in either standards development for a TDM call authentication framework or implement a robust robocall mitigation program as two options for satisfying the "reasonable measures" prong of this section. We agree as to the former suggestion, but we find the latter suggestion unduly overlaps with the distinct robocall mitigation program requirement under the statute.

117. We implement the provision in section 4(b)(2)(B)(ii) of the TRACED Act that voice service providers be "capable of fully implementing an effective caller ID authentication framework in the non-IP portions of their networks not later than [June 30, 2021]" by requiring that the voice service provider reasonably foresees that it will have completed all necessary network upgrades to its infrastructure to be able to authenticate and verify caller ID information for all non-IP calls originating or terminating on its network as provided by a standardized caller ID authentication framework for non-IP networks. This approach is consistent with our approach to the fourth prong of the IP network exemption, in which we construe "fully implementing" to mean that caller ID information is able to be authenticated and verified for *all* calls exchanged with technically-able partners. Further, it is consistent with our evaluation of

when a non-IP caller ID authentication framework is "reasonably available," and we consistently consider such a framework to be "effective" only when it is standardized. We find that this approach gives as much latitude to voice service providers as possible to achieve the desired result within the prescribed timeframe while again requiring some basis for the claim—here, that the provider be "capable of fully implementing an effective caller ID authentication framework."

4. Compliance Certifications

118. As proposed in the *Further Notice of Proposed Rulemaking*, we find that the best way to implement the TRACED Act's exemption provision is via a certification process. Specifically, we require a voice service provider that seeks to receive an exemption to submit a certification that it meets the criteria for the IP networks exemption that we have established pursuant to section 4(b)(2)(A), the criteria for the non-IP networks exemption that we have established pursuant to section 4(b)(2)(B), or both, as appropriate for its network(s). Given the inherent and obvious difficulty of making individualized determinations of whether providers qualify for the IP networks exemption on such a truncated timeframe, we find that a certification process is necessary to allow us to meet Congress's deadline for completion of exemption determinations by December 30, 2020. This approach is unopposed, and both T-Mobile and AT&T support the use of a certification process "as the appropriate vehicle for a voice service provider to assert its qualification for either or both of the statutory exemptions."

119. Each voice service provider that seeks to qualify for either the section 4(b)(2)(A) or the section 4(b)(2)(B) exemption, or both, must have an officer of the voice service provider sign a compliance certificate stating under penalty of perjury that the officer has personal knowledge that the company meets each of the stated criteria. Such an attestation is necessary to ensure the accuracy of the underlying certification. We also require the voice service provider to submit an accompanying statement explaining, in detail, how the company meets each of the prongs of each applicable exemption so that the Commission can verify the accuracy of the certification.

120. As proposed in the *Further Notice of Proposed Rulemaking*, all certifications submitted pursuant to this requirement must be filed no later than December 1, 2020. All certifications and supporting statements must be filed electronically in WC Docket No. 20-68, Exemption from Caller ID Authentication Requirements, in the Commission's Electronic Comment Filing System (ECFS). We direct the Bureau to provide additional directions and filing information regarding the certifications—including issuing protective orders governing the submission and review of confidential and highly confidential information, where necessary—by November 9, 2020, or in the Public Notice announcing Office of Management and Budget approval of this process, whichever comes sooner. And we direct the Bureau to review the certifications and accompanying documents for completeness and to determine whether the certifying party has met the requirements we have established. We further direct the Bureau to issue a list of parties that have filed complete, valid compliance certifications and that will thus receive the exemption(s) on or before December 30, 2020.

121. Because of the limited time for review of certifications, we proposed in the *Further Notice of Proposed Rulemaking* that any voice service providers that file inadequate certifications would not receive an opportunity to cure and instead would be subject to the general duty we established to implement STIR/SHAKEN by June 30, 2021. We adopt this proposal here. We find this consequence to be reasonable and appropriate because the purpose of the certification is merely to determine which voice service providers would, in the absence of the STIR/SHAKEN obligation, nonetheless be able to implement STIR/SHAKEN in a timely manner. While we are sympathetic to AT&T's suggestion that we permit voice service providers a chance to cure and revise their certifications should they be found deficient, the extremely truncated timeline for review of certifications prevents us from allowing such options. Simply put, there is insufficient time to permit voice service providers to revise and resubmit certifications that the Bureau has deemed deficient and for the Bureau to review such resubmitted certifications prior to the statutory December 30, 2020 deadline for completion of

exemption determinations. Voice service providers must do their best to demonstrate in their initial certifications that they have met all the statutory requirements necessary to qualify for an exemption. Moreover, as stated above, we find the inability of voice service providers to "cure" deficient certifications to be insignificant given the purpose of the certification.

122. *Implementation Verification*. The section 4(b)(2)(A) and (B) exemptions are, by their nature, based on a voice service provider's prediction of its future ability to implement STIR/SHAKEN by June 30, 2021. As we explained in the *Further Notice of Proposed Rulemaking*, we believe that Congress intended for us to verify, after the fact, that voice service providers claiming the exemption completed full implementation in accordance with their commitments. Such a review is consistent with the TRACED Act both because the broad structure of section 4 aims toward full implementation of caller ID authentication and because sections 4(b)(2)(A)(iv) and 4(b)(2)(B)(ii) each state that a voice service provider may receive the exemption only if it "will" be capable of "fully" implementing a caller ID authentication framework (STIR/SHAKEN or "an effective call authentication framework," respectively). This approach is unopposed in the record, and T-Mobile correctly notes that without such verification, the voluntary exemption could be misused as a loophole by voice service providers, thereby diminishing the ultimate effectiveness of STIR/SHAKEN implementation, the success of which depends on the participation of a critical mass of voice service providers. To guard against the risk of gaps and abusive claims of the exemption, and as proposed in the *Further Notice of Proposed Rulemaking*, we therefore require voice service providers that receive an exemption to file a second certification after June 30, 2021, stating whether they, in fact, achieved the implementation goal to which they previously committed.

123. As proposed in the *Further Notice of Proposed Rulemaking*, the certification must be filed electronically in WC Docket No. 20-68, Exemption from Caller ID Authentication Requirements, in ECFS subject to the same allowance for confidentiality and requirements for sworn signatures and detailed support as the initial certifications. This process will not only help

the Bureau to verify the accuracy of the certification, but will assist it in conducting its review while at the same time ensuring that any confidential or proprietary information included by filers remains safe from disclosure. We direct the Bureau to issue a Public Notice no later than three months after June 30, 2021, setting a specific deadline for the certifications and providing detailed filing requirements. We direct the Bureau to seek public comment on these certifications. Following review of the certifications, supporting materials, and responsive comments, we direct the Bureau to issue a Public Notice, no later than four months after the date of filing of the certifications, identifying which voice service providers achieved the implementation goal to which they previously committed. As suggested in the record, we clarify that voice service providers that certified in December of 2020 that they have already fully implemented the necessary STIR/SHAKEN requirements, and for which the Bureau accepted the certification, need not file a second certification. This second filing is required only from those voice service providers that have not yet "fully implemented" STIR/SHAKEN by the time of their initial December 2020 certification, but have committed to doing so by June 30, 2021.

124. We disagree with T-Mobile's assertion that there is little value is seeking public comment on voice service providers' certifications. While T-Mobile is correct that a review of whether a voice service provider has conformed to the terms of its exemption declarations and implemented STIR/SHAKEN will require a technical analysis, we anticipate that the considered comments of market participants, technical and trade associations, and industry professionals can inform and enrich the Bureau's analysis of any such technical issues. Further, allowing comments is critical to maintaining a clear and transparent process. Moreover, to the extent that parties must submit confidential information, the Bureau will issue protective orders governing submission and review akin to those we have employed in numerous other contexts. There is thus no risk that any voice service provider will be obligated to publicly disclose "sensitive network information" as part of this certification and comment process.

125. As proposed in the *Further Notice of Proposed Rulemaking*, if a voice service

provider cannot certify to full implementation upon the filing of the second certification but demonstrates to the Bureau that (1) it filed its initial certification in good faith—i.e., with a reasonable expectation that it would be able to achieve full implementation as certified—and (2) made similarly good faith efforts to complete implementation, the consequence for such a shortcoming is the loss of the exemption and application of the general rule requiring full STIR/SHAKEN implementation, effective immediately upon release of the Bureau Public Notice identifying which voice service providers achieved the implementation goal to which they previously committed. We find that an immediate effective date is required to ensure that certain voice service providers do not receive an extension not granted to similarly situated voice service providers simply because they filed a certification they later failed to meet. If the Bureau finds that a voice service provider filed its initial certification in bad faith or failed to take good faith steps toward implementation, we will not only require that voice service provider to fully implement STIR/SHAKEN immediately, but will further direct the Bureau to refer the voice service provider to the Enforcement Bureau for possible enforcement action based on filing a false initial certification.

5. Voice Service Providers Eligible for Exemption

126. We proposed in the *Further Notice of Proposed Rulemaking* to interpret the TRACED Act's exemption process to apply only to voice service providers and to exclude intermediate providers. We adopt that approach here. No commenters addressed this issue in the record. In the TRACED Act, Congress directs the Commission to require "provider[s] of voice service" to implement STIR/SHAKEN in the IP portions of their networks. The exemption provisions in section 4(b)(2) of the TRACED Act similarly refer to "provider[s] of voice service." Because the obligation on intermediate providers to implement the STIR/SHAKEN authentication framework is being adopted pursuant to our authority in the Truth in Caller ID Act and section 251(e), we do not believe that the exemption process, which is mandated under and governed by the TRACED Act, needs to apply to such intermediate

providers. We do not find that there is a compelling policy argument in favor of extending the TRACED Act's exemption process to intermediate providers. The exemption process as laid out in the TRACED Act will not have long-term benefits to providers, since even those that qualify for the exemption must be capable of fully implementing either the STIR/SHAKEN authentication framework or an effective call authentication framework not later than June 30, 2021. Given this, we are disinclined to add further administrative and regulatory complication where not required by the TRACED Act.

E. Line Item Charges

127. We adopt our proposal in the *First Caller ID Authentication Report and Order and FNPRM* to prohibit voice service providers from imposing additional line item charges on consumer or small business subscribers for caller ID authentication. The record reflects support for this proposal, and we believe adopting it is a straightforward implementation of Congress's direction and authority in the TRACED Act to "prohibit providers of voice service from adding any additional line item charges to consumer or small business customer subscribers for the effective call authentication technology."

128. We are unconvinced by arguments opposed to the rule we adopt in this document. MT Networks argues that we should instead affirmatively permit voice service providers to list caller ID authentication "as a billable feature on their line." Because MT Networks fails to explain how such an alternative course of action would be consistent with the text of the TRACED Act, we decline to adopt such a suggestion. Securus argues that the prohibition on line item charges should not apply to inmate calling service providers. We similarly decline to adopt such an exemption for these providers, as the TRACED Act's prohibition on line item charges extends to all "providers of voice service," which includes inmate calling service providers.

129. Other commenters argue that we should go even further than the TRACED Act and prohibit voice service providers from recouping costs of caller ID authentication and other robocall mitigation solutions entirely. Some commenters argue that we should also prohibit

charges for call blocking services. We decline to do so at this time because we do not address call blocking-related issues in this Report and Order. We decline to take such action because doing so would go beyond the directive in the TRACED Act, and because we recognize that implementation of caller ID authentication imposes cost on voice service providers. Additionally, the record shows that some voice service providers may not have enough resources simply to absorb the cost of implementing caller ID authentication. By not prohibiting cost recovery through alternate means, we promote the investment by all voice service providers in caller ID authentication solutions for their networks.

130. As proposed, we interpret "consumer" in this context to mean residential mass market subscribers, and adopt a rule consistent with this interpretation. We interpret "consumer" to refer to individual subscribers because we believe this interpretation will protect individuals from receiving line item charges on their bills. We received no opposition in the record to our proposal. We also adopt our proposal to interpret "small business" to refer to business entities that meet the Small Business Administration definition of "small business." We adopt this definition of "small business" because it reflects the judgment of the Small Business Administration, which has expertise in this area. We received no opposition in the record for this interpretation. We decline to adopt RadNet's proposal that we prohibit voice service providers "from charging healthcare facilities and providers, regardless of size, for call authentication technology," because the TRACED Act establishes the classes of entities that Congress intended to protect from additional line item charges for caller ID authentication: consumers and small business subscribers. Additionally, healthcare facilities that meet the standard for "small business" that we establish are covered by our rule, and so separate protection for such healthcare facilities would be redundant. Healthcare facilities that exceed the definition of "small business" are in a better position to negotiate billing arrangements with voice service providers than small businesses and residential mass market subscribers. Thus, providing them with the same protections would be unnecessary.

131. We also adopt our proposal to implement this section of the TRACED Act by prohibiting voice service providers from imposing a line item charge for the cost of upgrading network elements that are necessary to implement caller ID authentication, for any recurring costs associated with the authentication and verification of calls, or for any display of caller ID authentication information on their subscribers' phones. Caller ID authentication solutions work by allowing the originating voice service provider to authenticate the caller ID information transmitted with a call it originates, and the terminating provider to verify that the caller ID information transmitted with a call it receives is authentic and act on the information provided after verification. The record reflects that voice service providers must upgrade their existing network elements to enable caller ID authentication, and pay recurring maintenance and other operating fees in order to actively authenticate caller ID information. And, for caller ID authentication technology to be meaningful for subscribers, voice service providers may choose to display caller ID authentication information to their end users. We find that the prohibition as adopted covers the full scope of costs "for" providing caller ID authentication to consumer and small business subscribers.

132. CenturyLink argues that this is too expansive a reading of the TRACED Act's language. Instead, CenturyLink suggests that, to be more aligned with the language of the TRACED Act, we only prohibit line items for costs "related to the basic signing of calls and verifying of Identity headers." We fail to see how costs associated with, for example, network upgrades that are necessary to implement caller ID authentication are not "for" such technology, and CenturyLink does not explain why we should read "for" in this context so narrowly. We also note that we do not prohibit cost recovery for such costs by alternative means.

F. Intermediate Providers

133. To further promote effective, network-wide caller ID authentication, we adopt the proposal from our *First Caller ID Authentication Report and Order and FNPRM* to extend our STIR/SHAKEN implementation mandate to intermediate providers. The STIR/SHAKEN

framework enables an end-to-end system for authenticating the identity of the caller. For this system to work, the Identity header must travel the entire length of the call path—even when a call transits the networks of intermediate providers. Thus, intermediate providers play a crucial role in this system. In the *First Caller ID Authentication Report and Order and FNPRM*, we proposed imposing obligations on intermediate providers for calls they receive with authenticated and unauthenticated caller ID information. For calls with authenticated caller ID information that an intermediate provider receives and will exchange in SIP, we proposed requiring an intermediate provider to pass any Identity header associated with that call, unaltered, to the subsequent provider in the call path. And for calls an intermediate provider receives without authenticated caller ID information that it will exchange in SIP, we proposed requiring the intermediate provider to authenticate that call with "gateway" or "C"-level attestation before passing it to the subsequent intermediate or voice service provider in the call path. With modifications, we adopt both of these proposals.

1. Authenticated Calls

134. We adopt our proposal to require intermediate providers to pass any Identity header that they receive to the terminating voice service provider or subsequent intermediate provider in the call path. This means, technically, that the intermediate provider must forward the Identity header downstream in the SIP INVITE. By placing this requirement on intermediate providers, we ensure that SIP calls can benefit from STIR/SHAKEN regardless of what provider transits the call. This proposal received wide support, and no opposition, in the record. INCOMPAS, which notes that it represents a number of entities that act as intermediate providers, agrees that "[t]he success of STIR/SHAKEN ultimately depends on the broad participation of voice service providers, including, wherever technically feasible, intermediate providers." AT&T, Comcast, and Verizon also all confirm the importance of adopting this rule. AT&T notes that "requiring intermediate providers to pass through Identity header information is necessary to ensure that calls retain authentication information across the entire call path."

Comcast writes that "[a]chieving truly nationwide call authentication requires the participation of all providers involved in transmitting voice calls, including intermediate providers." And Verizon emphasizes that regulatory action is necessary to ensure intermediate provider involvement in the system. We agree with these assertions.

135. Additionally, we further adopt our proposal to require intermediate providers to pass the Identity header *unaltered*. We find that this requirement is necessary to prevent a downstream provider from tampering with the Identity header and thus undermining the end-to-end chain of trust between the originating and terminating voice service providers. Commenters support this approach, with NCTA stating that it is necessary to "maintain the integrity of the authentication information and reduce the potential for inadvertent error or intentional manipulation," and Hiya noting that "having access to untampered identity headers will significantly aid analytics and, as a result, the detection of illegal robocalls." This requirement ensures that all SIP calls benefit from STIR/SHAKEN, increasing the effectiveness of STIR/SHAKEN in combating illegally spoofed robocalls and fraudulent robocall schemes. And although entities acting as intermediate providers will face implementation costs in order to forward unaltered Identity headers, they will not face the recurring costs necessary to authenticate and verify caller ID information. Moreover, we expect these one-time implementation costs to be far less than the benefits of this intermediate provider requirement because the inclusion of intermediate providers is important to achieving the benefits discussed in the *First Caller ID Authentication Report and Order*. Requiring intermediate providers to pass the Identity headers that they receive to the subsequent intermediate provider in the call path or the terminating voice service provider is crucial to ensuring end-to-end caller ID authentication and unlocking these benefits for consumers and providers alike.

136. The record convinces us, however, to modify our proposal to allow an intermediate provider to strip the Identity header in two narrow circumstances: (1) for technical reasons where necessary to complete the call, and (2) for security reasons where an intermediate

provider reasonably believes the Identity header presents a threat to its network security. Several commenters explain that these are legitimate reasons why an intermediate provider might need to strip the Identity header.

137. In identifying the limited technical reasons an intermediate provider may need to strip the Identity header, the industry standards group ATIS explains that it may be necessary to strip an Identity header for call completion in cases such as Government Emergency Telecommunications Service (GETS) call processing; INCOMPAS identifies instances where the Identity header may be too large to successfully transit the network; and we recognize it may be necessary to strip the Identity header before exchanging a call with a non-IP provider or at a non-IP interconnection point. We emphasize that the technical necessity exception is narrow and limited to circumstances that are necessary to complete the call. The technical necessity exception does not extend to failures or inadequacies in an intermediate provider's network. As the technology supporting STIR/SHAKEN advances and improves, it may be possible to transmit headers in circumstances where it previously was not. As such, we will continue to monitor the use of this exception and adjust its outer limits as needed. Commission staff will not hesitate to refer reports of intermediate providers abuse of this exception to the Enforcement Bureau.

138. Regarding the security exception, Verizon advocates that we allow intermediate providers to act should Identity headers become "an attack vector used by bad actors." We agree and so do not prohibit an intermediate provider from stripping the Identity header when it reasonably believes the header presents an imminent threat to its network security. We do not, however, permit an intermediate provider to strip the header if it believes the Identity header has been tampered with or is fraudulent short of presenting an imminent security threat. This narrow exception does not empower the intermediate provider to make determinations on behalf of other providers in the call path or to interfere with the verification process defined in the SHAKEN standards. Instead, our goal is to permit an intermediate provider to act in the face of an

imminent security threat to its network. We emphasize that intermediate providers must employ this exception sparingly, and the exception will not apply where an intermediate provider strips Identity headers routinely instead of maintaining reasonable network security. Furthermore, since no commenter identified a circumstance where an intermediate provider would need to alter the Identity header, we specify that intermediate providers may not alter Identity headers under any circumstance.

139. Relatedly, we prohibit an originating voice service provider from sending excessively large headers with the goal of evading STIR/SHAKEN compliance by forcing an intermediate provider to strip the header before exchanging the call with a subsequent downstream provider. We would consider such conduct a violation of our rule requiring an originating voice service provider to authenticate caller ID information for calls it originates and exchanges with another voice service provider or intermediate provider.

140. ACA Connects proposes that we prohibit intermediate providers from passing a call they have received in SIP to a downstream provider in TDM when there is a downstream IP option available. We decline to adopt this proposal because, at this early stage, we do not wish to interfere with call routing decisions for the sake of promoting STIR/SHAKEN. Providers must consider a variety of factors when routing calls, including cost and reliability, and we do not believe at this stage that preserving STIR/SHAKEN headers should swamp all other considerations. For the same reason, we decline to adopt USTelecom's suggestion to require gateway providers to pass international traffic only to downstream providers that have implemented STIR/SHAKEN. Finally, while we do not require intermediate providers to append duplicative Identity headers to calls that they transit, we decline to prohibit this practice at this stage of STIR/SHAKEN deployment across the voice network. AT&T contends that, if intermediate providers append duplicative Identity headers, it would add additional complexity and consume bandwidth for other providers. However, this issue received little attention in the record and, at this time, we have no reason to think it is a practice industry will adopt widely.

We decline to be overly prescriptive at this early stage of deployment, and we will monitor this issue for any problems that develop.

2. Unauthenticated Calls

141. We also adopt a modified version of the proposed authentication requirement on intermediate providers for unauthenticated calls. Specifically, we require that an intermediate provider authenticate the caller ID information of a call that it receives with unauthenticated caller ID information that it will exchange with another intermediate provider or terminating voice service provider as a SIP call. However, a provider is relieved of this obligation if it (i) cooperatively participates with the industry traceback consortium and (ii) responds to all traceback requests it receives from the Commission, law enforcement, or the industry traceback consortium regarding calls for which it acts as an intermediate provider. Our final requirement differs from our proposed requirement in two ways. First, we do not require an intermediate provider to authenticate with a C-level or gateway attestation. Instead, if a provider chooses to authenticate the caller ID information of an unauthenticated call that it receives, we require only that a provider authenticate the caller ID information consistent with industry standards. And second, our modified requirement allows participation with the industry traceback consortium as an alternative option for compliance.

142. In the *First Caller ID Authentication Report and Order and FNPRM*, we proposed requiring intermediate providers to authenticate caller ID information for unauthenticated traffic that they receive with a C-level attestation, and tentatively concluded this requirement would improve traceback efforts and analytics. Some commenters—including major voice service providers that have reported substantial progress in STIR/SHAKEN implementation—endorse our reasoning that such a rule is in compliance with the industry standards, would enhance traceback capabilities, and would benefit call analytics. Neustar argues that intermediate providers should authenticate caller ID information for calls that they transmit that lack such information because "it allows the terminating voice service provider to more easily traceback

otherwise unauthenticated calls, and provides additional information that can be used to facilitate innovation in the robocall analytics space." And T-Mobile explains that intermediate provider authentication would be useful to terminating voice service providers because "[h]aving some information regarding this large subset of calls to enable traceback and strengthen analytics is preferable to having no information on which to make blocking and labeling decisions." T-Mobile further explains that even "C-attested calls all contain an origination ID ('origid')" which is "a globally unique identifier that represents the originating point of the call, such as the telephone switch where the call started, or a trunk group, which can be useful in tracing back the origin of a call." And T-Mobile notes that "[w]hile USTelecom's Industry Traceback Group ('ITG') can do its work without relying on origid, this does not obviate the need for origid, which would further advance ITG's goals."

143. We modify our proposal to require attestation consistent with industry standards rather than specifically requiring C-level attestation because this approach better aligns with our goal of promoting implementation of the industry-defined caller ID authentication standards rather than interfering with their technical application. This modification brings our intermediate provider rules in line with the STIR/SHAKEN obligations we imposed on originating and terminating voice service providers. In the *First Caller ID Authentication Report and Order and FNPRM*, we explained that for compliance with our rules it would be sufficient to adhere to the three standards that comprise the foundation of the STIR/SHAKEN framework—ATIS-1000074, ATIS-1000080, and ATIS-1000084—and all documents referenced therein. Recognizing that industry standards are not static, we framed the most recent versions of these standards as the baseline requirements for compliance. We follow that approach here and establish that compliance with the most current version of these three standards as of September 30, 2020, including any errata as of that date or earlier, represents the minimum requirement for intermediate providers to satisfy our rules. We encourage innovation and improvement to the STIR/SHAKEN framework, so long as any changes or additions do not compromise the baseline call authentication

functionality envisioned by ATIS-1000074, ATIS-1000080, and ATIS-1000084. An example of such an innovation is the recent technical report ATIS and the SIP Forum released providing guidelines for originating providers on the population of the SHAKEN attestation indicator and origination identifier.

144. Beyond harmonizing our requirements on intermediate providers and originating and terminating voice service providers, this modification responds to record interest in allowing, where possible, intermediate providers to authenticate caller ID information with a higher level of attestation than a C-level attestation. It is not our intent to preclude or interfere with efforts to accommodate this interest; only to ensure the caller ID information for such calls be authenticated. To that end, we agree with commenters that argue we should not require intermediate providers to authenticate calls with a specific level of attestation, and require instead that intermediate providers authenticate the caller ID information for unauthenticated calls consistent with industry standards as described above. This clarification allows for and encourages industry progress, and we look forward to seeing progress on the numerous proposals in the record to allow for more robust authentication of such calls. We decline to require any specific solution, as some commenters suggest, or to impose a specific timeline. We encourage interested parties to continue this work promptly, but the record does not include enough information on which to base a deadline, and industry standards bodies are better-suited to modify the standards they have created.

145. Although we establish this requirement, in response to arguments that our proposal was unduly burdensome in some cases, we allow for an intermediate provider to register and participate with the industry traceback consortium as an alternative means of complying with our rules. Several commenters claim that a requirement for intermediate providers to authenticate the caller ID information of all unauthenticated calls that they receive would cause bandwidth problems within provider networks. Several commenters also express concern that an attestation requirement would undermine the efficacy of STIR/SHAKEN by

"pollut[ing] the ecosystem" with "billions of useless attestations," causing customer harm and confusion. Further, some commenters contend that such a requirement would not lead to the benefits that we proposed would accrue. Other commenters in the record push back on these concerns, and because of the potential value of more ubiquitous authentication, we do not find that these concerns justify the elimination of this requirement entirely. We find that attestation of previously unauthenticated calls will provide significant benefits in facilitating analytics, blocking, and traceback by offering all parties in the call ecosystem more information, and we thus allow attestation of unauthenticated calls as one method for compliance. This conclusion is consistent with our analysis in the *First Caller ID Authentication Report and Order*, where we found that the benefits of requiring providers to authenticate calls will substantially outweigh the costs.

146. While we make this conclusion, we acknowledge record concerns about the cost of requiring intermediate provider authentication and thus offer an alternative method of compliance that we anticipate will be less burdensome and will nonetheless facilitate traceback of calls. Specifically, establish that an entity acting as an intermediate provider is relieved of the requirement to authenticate the caller ID information of unauthenticated calls it receives if it (i) cooperatively participates with the industry traceback consortium, and (ii) responds to all traceback requests it receives from the Commission, law enforcement, or the industry traceback consortium for calls for which it acts as an intermediate provider. We again underscore that this requirement does not supersede any existing legal processes, and we encourage law enforcement to make traceback requests through the industry traceback consortium.

147. Providing this option addresses intermediate provider concerns over the burden that an authentication requirement would place on their networks. It further allows for continued evaluation of the role intermediate providers play in authenticating the caller ID information of the unauthenticated calls that they receive amid the continued deployment of the STIR/SHAKEN framework. By ensuring that all calls which transit the voice network either receive some form

of attestation or are carried by an intermediate provider that is registered with the industry traceback consortium, terminating voice service providers will have more data about a call that can be used to support traceback efforts and call analytics, and prevent future illegal robocalls—further increasing the net benefits offered by STIR/SHAKEN. Additionally, providing this option for intermediate providers aligns with the robocall mitigation requirements we adopt in this document. By requiring intermediate providers and many originating voice service providers to engage in practices that promote traceback, we will ensure broad participation through the entire call path to determine the source of illegal robocalls. Although the obligation to either authenticate or participate in the industry traceback consortium with respect to unauthenticated calls will place costs on intermediate providers, we have no reason to believe that our additional mandate will fundamentally disturb our cost-benefit calculus for STIR/SHAKEN implementation. AT&T argues that "[t]he initial estimates of the major providers' costs to implement STIR/SHAKEN grossly underestimate reality," and that STIR/SHAKEN implementation costs "easily will exceed hundreds of millions of dollars." We are not convinced by this assertion as AT&T does not provide concrete evidence to support such claims, nor any explanation as to why initial estimates were inaccurate.

148. We find it unnecessary to adopt CTIA's suggestion to require intermediate providers serving as international gateways to register with the Commission. Under the rules we adopt, such providers are required either to authenticate the caller ID information of the foreign-originated calls that they receive and will transit on their networks or to register with the industry traceback consortium and participate in traceback efforts. Both options we adopt address call tracing more directly than a mere registration requirement, and we are reluctant to create multiple overlapping registration requirements for providers that choose the latter option. We can revisit CTIA's suggestion should the measures we adopt prove insufficient.

3. Limiting Intermediate Provider Requirements to IP Networks

149. In the *First Caller ID Authentication Report and Order and FNPRM*, we

proposed limiting our caller ID authentication obligations on intermediate providers to IP calls. We adopt our proposal with modifications. First, we adopt this proposal for calls with authenticated caller ID information that an intermediate provider receives. In so doing, we limit the requirement that intermediate providers pass any received Identity header unaltered to IP calls, that is, calls that the intermediate provider receives in SIP and exchanges with a terminating provider or another intermediate provider in SIP. Commenters support limiting our rule to IP calls, and doing so harmonizes our rules for intermediate providers with our rules applying to originating and terminating voice service providers.

150. Second, we modify this proposal for calls with unauthenticated caller ID information that an intermediate provider receives. To the extent that an intermediate provider chooses to comply with the rules we adopt in this document by authenticating the caller ID information of the unauthenticated calls that it receives, as Comcast suggests, we clarify that this requirement applies to *all* unauthenticated calls an intermediate provider receives that it will exchange with a subsequent provider in SIP, regardless of whether the intermediate provider receives the call in SIP. In other words, if the intermediate provider chooses to authenticate the caller ID information of unauthenticated calls, the obligation applies if the intermediate provider transmits the call downstream in SIP. We make this modification in recognition of the fact that calls without authenticated caller ID information may have originated on non-IP networks or have been exchanged at non-IP interconnection points and thus do not have an existing Identity header. In those instances, the obligation to authenticate the caller ID information according to industry standards applies whether or not the call was received by the intermediate provider in SIP.

151. We decline to adopt Comcast's proposal that intermediate providers exchanging traffic in TDM install TDM-to-VoIP gateways. At this time, we believe that such a requirement would be unduly burdensome. Furthermore, it would go beyond both Congress's and our approach to addressing the issues around non-IP technology and caller ID authentication, which aim to strike a balance between encouraging the IP transition and the development of non-IP

solutions for the benefit of those networks that cannot be speedily or easily transitioned. We will continue to monitor the development of technical solutions to the issue of TDM exchange and are prepared to return to this proposal if circumstances warrant.

4. Definition of Intermediate Provider

152. We adopt our proposal from the *First Caller ID Authentication Report and Order and FNPRM* to use the definition of "intermediate provider" found in § 64.1600(i) of our rules. This section provides that an "intermediate provider" is "any entity that carries or processes traffic that traverses or will traverse the [PSTN] at any point insofar as that entity neither originates nor terminates that traffic." We further determine that as with our interpretation of "providers of voice service," we assess the definition of "intermediate provider" on a call-by-call basis for the purpose of our call authentication rules. A single entity therefore may act as a voice service provider for some calls on its network and an intermediate provider for others. Intermediate providers play a critical role in ensuring end-to-end call authentication. We believe that this broad definition will best promote the widespread deployment of the STIR/SHAKEN framework that is necessary to benefit consumers.

153. We sought comment in the *First Caller ID Authentication Report and Order and FNPRM* on whether we should use a narrower definition of intermediate provider, such as the one we use in the context of rural call completion. One commenter advocates for a narrower definition that would "not include in its scope an ISP that is only incidentally transmitting voice traffic," because this "could place a substantial burden on small, rural ISPs transmitting Non-Interconnected VoIP or Interconnected VoIP via a third-party service provider they have no relationship with." As we explained in the *First Caller ID Authentication Report and Order and FNPRM*, the STIR/SHAKEN framework relies on the transmission of information in the Identity header of a SIP INVITE. We understand that there are circumstances where a call set up using SIP signaling will then use other paths to exchange the media packets containing voice data. Because we have limited our rules to the exchanging of SIP calls, to the extent that an ISP is only

transmitting voice traffic of a call that does not involve the exchange of a SIP INVITE, we believe it is already excluded from our rules.

5. Legal Authority

154. We find that we have the authority to place caller ID authentication obligations on intermediate providers and alternatively to require that they register and participate with the industry traceback consortium under section 251(e) of the Act. In the *First Caller ID Authentication Report and Order*, we concluded that our exclusive jurisdiction over numbering policy provides authority to require voice service providers to implement STIR/SHAKEN in order to prevent the fraudulent abuse of NANP resources. In the *FNPRM*, we proposed that this same analysis provides the Commission authority to impose STIR/SHAKEN implementation requirements on intermediate providers. Several commenters support this view. Calls that transit the networks of intermediate providers with illegally spoofed caller ID are exploiting numbering resources in the same manner as spoofed calls on the networks of originating and terminating providers, and so we find authority under section 251(e). Consistent with the *First Caller ID Authentication Report and Order and FNPRM*, we adopt our proposal concluding that the section 251(e)(2) requirements do not apply in the context of our establishing STIR/SHAKEN requirements. Because STIR/SHAKEN implementation is not a "numbering administration arrangement," section 251(e)(2), which provides that "[t]he cost of establishing telecommunications numbering administration arrangements . . . shall be borne by all telecommunications carriers on a competitively neutral basis," does not apply here. Even if section 251(e)(2) does apply, we conclude that because each carrier is responsible for bearing its own implementation costs, the requirement is satisfied. Each carrier's costs will be proportional to the size and quality of its network.

155. We find additional, independent authority under the Truth in Caller ID Act. The Truth in Caller ID Act charged the Commission with prescribing rules to make unlawful the spoofing of caller ID information "in connection with any voice service or text messaging

service . . . with the intent to defraud, cause harm, or wrongfully obtain anything of value." We agree with T-Mobile that this provides us with authority to mandate that intermediate providers adopt "a framework that will minimize the frequency with which illegally spoofed scam calls will reach consumers." We found authority in the *First Caller ID Authentication Report and Order* for our STIR/SHAKEN implementation mandate on originating and terminating voice service providers under the Truth in Caller ID Act. We explained that "the rules we adopt today are necessary to enable voice service providers to help prevent these unlawful acts and to protect voice service subscribers from scammers and bad actors." That same analysis applies to intermediate providers that, as noted, play an integral role in the success of STIR/SHAKEN across the voice network.

156. Verizon, the only commenter to challenge our legal authority, argues that we lack authority under either section 251(e) or the Truth in Caller ID Act to require an intermediate provider to authenticate with a C-level attestation the caller ID information for unauthenticated calls it receives. It asserts that "'C' attestations do not attest to the accuracy of numbers and indeed have nothing to do with numbering resources," and consequently that section 251(e) does not provide us with authority; it further argues that "'C' attestations have nothing to do with the spoofing problem" and so could not be required under the Truth in Caller ID Act. Verizon also argues that we may not "go beyond the scope of the legal authority granted by the TRACED Act," but overlooks language in that very Act providing that "[n]othing in this section shall preclude the Commission from initiating a rulemaking pursuant to its existing statutory authority." As an initial matter, Verizon's objections are less pressing because of the modifications we made to our final rule—requiring only authentication consistent with industry standards *or* registration and participation with the industry traceback consortium. Furthermore, we do not agree that C-level attestations "have nothing to do with" numbering resources or spoofing. The STIR/SHAKEN standards expressly include the option of C-level attestation, and we think it apparent that this component of "a technology specifically designed to counteract

misuse of numbering resources" through spoofing relates both to our authority under section 251(e) and the Truth in Caller ID Act. When bad actors unlawfully falsify or spoof the caller ID that appears on a subscriber's phone, they are using numbering resources to advance an illegal scheme. Mandating that intermediate providers authenticate unauthenticated calls or participate in traceback efforts will help to prevent and remediate the fraudulent exploitation of NANP resources and illegal spoofing of caller ID information.

G. Other Issues

157. *No Additional Exceptions from Originating Voice Service Provider Caller ID Authentication Mandate*. We reject the record requests to grant limited exceptions from our caller ID authentication rules. We construe these requests, which do not respond to any part of the *FNPRM*, as petitions for reconsideration of the rules adopted in the *First Caller ID Authentication Report and Order and FNPRM*. Verizon argues that we should free a voice service provider from our caller ID authentication rules in certain circumstances where, in its view, it would be "inadvisable or inappropriate for the originating carrier to place a signature on a call." Verizon, USTelecom, and CTIA argue that these circumstances include "periods of substantial network congestion," such as national emergencies or natural disasters, or during periods of network maintenance. Verizon further argues that a voice service provider should not be required to authenticate caller ID information in certain complicated calling cases. We decline to grant these categorical exceptions from our mandate. Our goal is ubiquitous deployment of caller ID authentication technology, and no commenter explains with specificity why its concerns outweigh that goal. To the contrary, national emergencies and natural disasters are among the times when caller ID authentication is most important. In those instances, affected individuals must be able to rely on the caller ID information they receive and avoid bad actors taking advantage of an ongoing emergency or its aftermath. And while we do not grant an exception for complicated calling cases, we underscore that, to the extent a certain calling case is not accounted for by industry standards, application of caller ID authentication is not called for

by our rules. We explained in the *First Caller ID Authentication Report and Order* that "[c]ompliance with the most current versions of . . . three standards as of March 31, 2020, including any errata as of that date or earlier, represents the minimum requirement to satisfy our rules." USTelecom and CTIA argue that, because we provide intermediate providers limited exceptions to our requirement that they transit Identity headers unaltered, we must also provide an exception for originating voice service providers from our call authentication mandate. But these commenters fail to explain why adopting narrowly tailored exceptions for intermediate providers justifies adopting the far broader exception that they seek. Beyond generalized concerns over network congestion and maintenance, no commenter provides a specific technical rationale for when originating voice service providers should receive an exception from our caller ID authentication requirements.

158. *Non-Substantive Rule Revision*. We revise § 64.6301(a)(2) of our rules to make two non-substantive changes. First, the adopted rule inadvertently omitted the word "it." Second, the adopted rule referred to "caller ID authentication information," inconsistent with other terms in the rules. The rule as revised provides that a voice service provider shall "authenticate caller identification information for all SIP calls it originates and that *it* will exchange with another voice service provider or intermediate provider and, to the extent technically feasible, transmit that call with *authenticated caller identification information* to the next voice service provider or intermediate provider in the call path." We make these revisions without seeking notice and comment pursuant to section 553(b)(3)(B) of the Administrative Procedure Act, which states that an agency for good cause may dispense with rulemaking if it finds that notice and comment are "impracticable, unnecessary, or contrary to the public interest." Here, notice and comment are unnecessary because correcting the rule does not have a detrimental effect on the parties regulated by rule and does not alter the regulatory framework established by the *First Caller ID Authentication Report and Order*.

IV. PROCEDURAL MATTERS

159. *Final Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act of 1980 (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *First Caller ID Authentication Report and Order and FNPRM*. The Commission sought written public comment on the possible significant economic impact on small entities regarding the proposals addressed in the *First Caller ID Authentication Report and Order and FNPRM*, including comments on the IRFA. No comments were filed addressing the IRFA. This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this *Second Report and Order*, including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).

A. Need for, and Objectives of, the Rules

160. In this *Second Report and Order* (*Order*), we continue the Commission's efforts to combat illegal spoofed robocalls. Specifically, the *Order* implements the provisions of section 4 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act as follows: requiring providers to take "reasonable measures" to implement an effective caller ID authentication framework in their non-IP networks by either completely upgrading non-IP networks to IP or by actively working to develop a non-IP authentication solution; granting extensions of varying lengths from implementation of caller ID authentication for (1) small, including small rural, voice service providers; (2) voice service providers that cannot obtain a certificate due to the Governance Authority's token access policy until such provider is able to obtain a certificate; (3) services scheduled for section 214 discontinuance; and (4) as required by the TRACED Act, an extension for the parts of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls until a solution for such calls is reasonably available; granting an exemption from our implementation mandate for providers which have certified that they have reached certain implementation goals; and prohibiting providers from imposing additional line item charges on consumer and small

business subscribers for caller ID authentication technology. The *Order* also adopts rules requiring intermediate providers to (1) pass any Identity header that they receive to the terminating voice service provider or subsequent intermediate provider in the call path; and (2) either (i) authenticate the caller ID information of a call that it receives with unauthenticated caller ID information that it will exchange with another intermediate provider or terminating voice service provider as a SIP call, or (ii) cooperatively participate with the Commission-selected consortium to conduct traceback efforts. These rules will help promote effective caller ID authentication and fulfill our obligations under the TRACED Act.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

161. There were no comments filed that specifically addressed the proposed rules and policies presented in the IRFA.

C. Response to Comments by the Chief Counsel for Advocacy of the SBA

162. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.

163. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

164. The RFA directs agencies to provide a description and, where feasible, an estimate of the number of small entities that may be affected by the final rules adopted pursuant to the *Order*. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small-business concern"

under the Small Business Act. A "small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

1. Wireline Carriers

165. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry." The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees. Thus, under this size standard, the majority of firms in this industry can be considered small.

166. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated for the entire year. Of that total, 3,083 operated with fewer than 1,000 employees. Thus under this category and the associated size standard, the Commission estimates that the majority of local exchange carriers

are small entities.

167. *Incumbent Local Exchange Carriers (incumbent LECs).* Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated the entire year. Of this total, 3,083 operated with fewer than 1,000 employees. Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers. Of this total, an estimated 1,006 have 1,500 or fewer employees. Thus, using the SBA's size standard the majority of incumbent LECs can be considered small entities.

168. *Competitive Local Exchange Carriers (Competitive LECs), Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate NAICS Code category is Wired Telecommunications Carriers and under that size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees. Based on these data, the Commission concludes that the majority of Competitive LECS, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers, are small entities. According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services. Of these 1,442 carriers, an estimated 1,256 have 1,500 or fewer employees. In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or

fewer employees. Also, 72 carriers have reported that they are Other Local Service Providers. Of this total, 70 have 1,500 or fewer employees. Consequently, based on internally researched FCC data, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.

169. We have included small incumbent LECs in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small-business size standard (e.g., a telephone communications business having 1,500 or fewer employees) and "is not dominant in its field of operation." The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not "national" in scope. We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

170. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers. The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year. Of that number, 3,083 operated with fewer than 1,000 employees. According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services. Of this total, an estimated 317 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of interexchange service providers are small entities.

171. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended, also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one

percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000." As of 2019, there were approximately 48,646,056 basic cable video subscribers in the United States. Accordingly, an operator serving fewer than 486,460 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate. Based on available data, we find that all but five cable operators are small entities under this size standard. We note that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

2. Wireless Carriers

172. *Wireless Telecommunications Carriers (except Satellite).* This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed of 1000 employees or more. Thus under this category and the associated size standard, the Commission estimates that the majority of Wireless Telecommunications Carriers (except Satellite) are small entities.

173. The Commission's own data—available in its Universal Licensing System—indicate that, as of August 31, 2018 there are 265 Cellular licensees that will be affected by our actions. The Commission does not know how many of these licensees are small, as the

Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services. Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500 employees. Thus, using available data, we estimate that the majority of wireless firms can be considered small.

174. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications." Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules. For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year. Of this total, 299 firms had annual receipts of less than $25 million. Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

3. Resellers

175. *Local Resellers.* The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. Under the SBA's size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data from 2012 show that 1,341 firms provided resale services during that year. Of that number, all

operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services. Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees. Consequently, the Commission estimates that the majority of local resellers are small entities.

176. *Toll Resellers.* The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees. 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services. Of this total, an estimated 857 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of toll resellers are small entities.

177. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business definition specifically for prepaid calling card providers. The most appropriate NAICS code-based category for defining prepaid calling card providers is Telecommunications Resellers. This industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and

reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual networks operators (MVNOs) are included in this industry. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these prepaid calling card providers can be considered small entities. According to the Commission's Form 499 Filer Database, 86 active companies reported that they were engaged in the provision of prepaid calling cards. The Commission does not have data regarding how many of these companies have 1,500 or fewer employees, however, the Commission estimates that the majority of the 86 active prepaid calling card providers that may be affected by these rules are likely small entities.

4. Other Entities

178. *All Other Telecommunications.* The **"**All Other Telecommunications" category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry. The SBA has developed a small business size standard for "All Other Telecommunications", which consists of all such firms with annual receipts of $35 million or less. For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year. Of those firms, a total of 1,400 had annual receipts less than $25 million and 15 firms had annual receipts of $25

million to $49, 999,999. Thus, the Commission estimates that the majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

179. The *Order* adopts rules that obligate voice service providers that use non-IP network technology to be able to provide the Commission, upon request, with documented proof that the provider is participating, either on its own or through a representative, as a member of a working group, industry standards group, or consortium that is working to develop a non-IP solution, or actively testing such a solution. Under this rule, a voice service provider satisfies its obligations if it participates through a third-party representative, such as a trade association of which it is a member or vendor.

180. Section 4(b)(5)(C)(i) of the TRACED Act directs the Commission to require any voice service provider that has been granted an extension in compliance with the caller ID authentication implementation mandates to implement, during the time of the extension, "an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider." The *Order* requires voice service providers to file certifications documenting and describing their robocall mitigation programs. Specifically, the *Order* requires all voice service providers—not only those granted an extension—to certify on or before June 30, 2021, that their traffic is either signed with STIR/SHAKEN or subject to a robocall mitigation program that includes taking reasonable steps to avoid originating illegal robocall traffic, and committing to cooperating with law enforcement and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls. For those voice service providers that certify that some or all of their traffic is subject to a robocall mitigation program, the *Order* requires such voice service providers to detail in their certifications the specific "reasonable steps" that they have taken to avoid originating illegal robocall traffic. While only voice service providers with an extension will be

obligated to implement a robocall mitigation program, the *Order* imposes the certification requirement on all voice service providers because doing so will help the Commission and others to hold all voice service providers accountable for the voice traffic they originate, and give the Commission and others a snapshot of the progress of STIR/SHAKEN implementation and the variety of robocall mitigation practices adopted by voice service providers.

181. Voice service providers must file robocall mitigation certifications via a portal on the Commission's website that we will establish for this purpose. The *Order* also requires voice service providers filing certifications to provide the following identification information in the portal on the Commission's website:

(1) the voice service provider's business name(s) and primary address;

(2) other business names in use by the voice service provider;

(3) all business names previously used by the voice service provider;

(4) whether a voice service provider is a foreign voice service provider; and

(5) the name, title, department, business address, telephone number, and email address of a central point of contact within the company responsible for addressing robocall-mitigation-related issues.

182. The *Order* also requires voice service providers to submit to the Commission any necessary updates regarding any of the information they filed in the certification process within 10 business days. The *Order* extends this certification requirement to foreign voice service providers that use U.S. North American Numbering Plan numbers that pertain to the United States to send voice traffic to residential and business subscribers in the United States and wish to be listed in the database.

183. The *Order* also adopts rules in accordance with our proposal to require that, in order to receive a voluntary exemption from our implementation mandate, a voice service provider must file a certification reflecting that it is in a reasonably foreseeable position to meet certain implementation goals, and that, in order to maintain that exemption, a provider must

make a later filing reflecting its achievement of those goals it stated it was in a reasonably foreseeable position to meet. The requirement of such certifications entails new reporting, recordkeeping, and other compliance requirements for voice service providers. Specifically, we require that each voice service provider that wishes to qualify for the voluntary exemption from our implementation mandate must have an officer of the voice service provider sign a compliance certificate stating, under penalty of perjury, that the officer has personal knowledge that the company meets each of the stated criteria. We also require the voice service provider to submit an accompanying statement explaining, in detail, how the company meets each of the prongs of each applicable exemption so that the Commission can verify the accuracy of the certification. We also require that these certifications be filed no later than December 1, 2020, and that all certifications and supporting statements be filed electronically in WC Docket No. 20-68, Exemption from Caller ID Authentication Requirements, in the Commission's Electronic Comment Filing System (ECFS). Voice service providers that receive an exemption are further required to file a second certification by a deadline specified in a Public Notice issued by the Wireline Competition Bureau no later than three months after June 30, 2021, stating whether they, in fact, achieved the implementation goal to which they previously committed. The certification must be filed electronically in WC Docket No. 20-68, Exemption from Caller ID Authentication Requirements, in ECFS subject to the same allowance for confidentiality and requirements for sworn signatures and detailed support as the initial certifications. Voice service providers that certified in December of 2020 that they have already fully implemented the necessary STIR/SHAKEN requirements, and for which the Bureau accepted the certification, need not file a second certification. This second filing is required only from those voice service providers that have not yet "fully implemented" STIR/SHAKEN by the time of their initial December 2020 certification, but have committed to doing so by June 30, 2021.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

184. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof for such small entities."

185. The rules we adopt in this *Order* permit providers to satisfy the requirement under section 4(b)(1)(B) of the TRACED Act to take "reasonable measures" to implement an effective caller ID authentication framework in the non-IP portions of their networks, by participating as a member of a working group, industry standards group, or consortium that is working to develop a non-IP solution, or actively testing such a solution. A voice service provider satisfies this obligation if it participates through a third-party representative, such as a trade association of which it is a member or vendor. As the record in this proceeding shows, some industry groups have already established working groups dedicated to examining potential non-IP call authentication technologies. Allowing for such representatives will reduce the burden of this obligation on individual voice service providers, including those which are smaller, and minimize the potential negative impact of broad and inexpert participation identified in the record, while ensuring that all voice service providers remain invested in developing a solution for non-IP caller ID authentication.

186. In addition, the *Order* grants a two-year extension from implementation of caller ID authentication to small, including small rural, voice service providers. The *Order* also grants an exemption from our implementation mandate for voice service providers, including small providers, which certify that they have reached certain implementation goals, and prohibits voice service providers from imposing additional line item charges on consumer or small business

subscribers for caller ID authentication. In these ways, we have taken steps to minimize the economic impact of the rules adopted in this *Order* on small entities.

Report to Congress:

187. The Commission will send a copy of the *Order*, including this FRFA, in a report to Congress pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the *Order*, including this FRFA, to the Chief Counsel for Advocacy of the SBA.

188. *Paperwork Reduction Act*. This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, we previously sought comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

189. *Congressional Review Act*. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs that this rule is "non-major" under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this *Second Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

V. ORDERING CLAUSES

190. Accordingly, IT IS ORDERED, pursuant to sections 4(i), 4(j), 227(e), 227b, 251(e), and 303(r), of the Communications Act of 1934, as amended (the Act), 47 U.S.C. 154(i), 154(j), 227(e), 227b, 251(e), and 303(r), that this *Second Report and Order* IS ADOPTED.

191. IT IS FURTHER ORDERED that part 64 of the Commission's rules IS AMENDED as set forth in the Final Rules, and that any such rule amendments that contain new

or modified information collection requirements that require approval by the Office of Management and Budget under the Paperwork Reduction Act SHALL BE EFFECTIVE after announcement in the **Federal Register** of Office of Management and Budget approval of the rules, and on the effective date announced therein.

192. IT IS FURTHER ORDERED that, pursuant to §§ 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR 1.4(b)(1), 1.103(a), this *Second Report and Order* SHALL BE EFFECTIVE 30 days after publication in the **Federal Register**, except for the addition of §§ 64.6303(b) and 64.6305(b), to the Commission's rules that have not been approved by OMB. The Federal Communications Commission will publish documents in the **Federal Register** announcing the effective dates of these provisions.

193. IT IS FURTHER ORDERED that the Commission SHALL SEND a copy of this *Report and Order* to Congress and to the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. 801(a)(1)(A).

194. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Second Report and Order*, including the Final Regulatory Flexibility Analysis (FRFA), to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Part 64

Common carriers.

FEDERAL COMMUNICATIONS COMMISSION.

Marlene Dortch,
Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR part 64 as follows:

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

1. The authority citation for part 64 continues to read as follows:

AUTHORITY: 47 U.S.C. 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 262, 403(b)(2)(B), (c), 616, 620, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091.

2. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, amend § 64.6300 by redesignating paragraphs (e) through (g) as paragraphs (j) through (l) and paragraphs (c) and (d) as paragraphs (f) and (h), respectively, and adding new paragraphs (c) through (e), (g), and (i) to read as follows:

§ 64.6300 Definitions.

* * * * *

(c) *Foreign voice service provider*. The term "foreign voice service provider" refers to any entity providing voice service outside the United States that has the ability to originate voice service that terminates in a point outside that foreign country or terminate voice service that originates from points outside that foreign country.

(d) *Governance Authority*. The term "Governance Authority" refers to the Secure Telephone Identity Governance Authority, the entity that establishes and governs the policies regarding the issuance, management, and revocation of Service Provider Code (SPC) tokens to intermediate providers and voice service providers.

(e) *Industry traceback consortium*. The term "industry traceback consortium" refers to the consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls as selected by the Commission pursuant to § 64.1203.

* * * * *

(g) *Robocall Mitigation Database.* The term "Robocall Mitigation Database" refers to a database accessible via the Commission's website that lists all entities that make filings pursuant to § 64.6305(b).

* * * * *

(i) *SPC token*. The term "SPC token" refers to the Service Provider Code token, an authority token validly issued to an intermediate provider or voice service provider that allows the provider to authenticate and verify caller identification information consistent with the STIR/SHAKEN authentication framework in the United States.

* * * * *

3. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, amend § 64.6301 by revising paragraphs (a) introductory text and (a)(2) to read as follows:

§ 64.6301 Caller ID authentication.

(a) *STIR/SHAKEN implementation by voice service providers.* Except as provided in §§ 64.6304 and 64.6306, not later than June 30, 2021, a voice service provider shall fully implement the STIR/SHAKEN authentication framework in its Internet Protocol networks. To fulfill this obligation, a voice service provider shall:

* * * * *

(2) Authenticate caller identification information for all SIP calls it originates and that it will exchange with another voice service provider or intermediate provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path; and

* * * * *

4. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, add § 64.6302 to read as follows:

§ 64.6302 Caller ID authentication by intermediate providers.

Not later than June 30, 2021, each intermediate provider shall fully implement the STIR/SHAKEN authentication framework in its Internet Protocol networks. To fulfill this obligation, an intermediate provider shall:

(a) Pass unaltered to the subsequent intermediate provider or voice service provider in the call path any authenticated caller identification information it receives with a SIP call, subject to the following exceptions under which it may remove the authenticated caller identification information:

(1) Where necessary for technical reasons to complete the call; or

(2) Where the intermediate provider reasonably believes the caller identification authentication information presents an imminent threat to its network security; and

(b) Authenticate caller identification information for all calls it receives for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, except that the intermediate provider is excused from such duty to authenticate if it:

(1) Cooperatively participates with the industry traceback consortium; and

(2) Responds fully and in a timely manner to all traceback requests it receives from the Commission, law enforcement, and the industry traceback consortium regarding calls for which it acts as an intermediate provider.

5. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, add § 64.6303 to read as follows:

§ 64.6303 Caller ID authentication in non-IP networks.

Except as provided in §§ 64.6304 and 64.6306, not later than June 30, 2021, a voice service provider shall:

(a) Upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6301 throughout its network.

(b) [Reserved]

6. Delayed indefinitely, amend § 64.6303 by:

a. Adding the word "either" at the end of the introductory text;

b. Removing the period at the end of paragraph (a) and adding "; or" in its place; and

c. Adding paragraph (b).

The addition reads as follows:

§ 64.6303 Caller ID authentication in non-IP networks.

* * * * *

(b) Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-Internet Protocol caller identification authentication solution, or actively testing such a solution.

7. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, add § 64.6304 to read as follows:

§ 64.6304 Extension of implementation deadline.

(a) *Small voice service providers*. (1) Small voice service providers are exempt from the requirements of § 64.6301 through June 30, 2023.

(2) For purposes of this paragraph (a), "small voice service provider" means a provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the provider's affiliates).

(b) *Voice service providers that cannot obtain a SPC token*. Voice service providers that are incapable of obtaining a SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining a SPC token.

(c) *Services scheduled for section 214 discontinuance.* Services which are subject to a

pending application for permanent discontinuance of service filed as of June 30, 2021, pursuant to the processes established in 47 CFR 63.60 through 63.100, as applicable, are exempt from the requirements of § 64.6301 through June 30, 2022.

(d) *Non-IP networks.* Those portions of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of § 64.6303 as to the portion of its network subject to the extension.

(e) *Provider-specific extensions.* The Wireline Competition Bureau may extend the deadline for compliance with § 64.6301 for voice service providers that file individual petitions for extensions by November 20, 2020. The Bureau shall seek comment on any such petitions and issue an order determining whether to grant the voice service provider an extension no later than March 30, 2021.

(f) *Annual reevaluation of granted extensions.* The Wireline Competition Bureau shall, in conjunction with an assessment of burdens and barriers to implementation of caller identification authentication technology, annually review the scope of all previously granted extensions and, after issuing a Public Notice seeking comment, may extend or decline to extend each such extension, and may decrease the scope of entities subject to a further extension.

8. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, add § 64.6305 to read as follows:

§ 64.6305 Robocall mitigation and certification.

(a) *Robocall mitigation program requirements.* (1) Any voice service provider subject to an extension granted under § 64.6304 that has not fully implemented the STIR/SHAKEN authentication framework on its entire network shall implement an appropriate robocall mitigation program as to those portions of its network on which it has not implemented the STIR/SHAKEN authentication framework.

(2) Any robocall mitigation program implemented pursuant to paragraph (a)(1) of this

section shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

(b) - (c) [Reserved]

9. Delayed indefinitely, amend § 64.6305 by adding paragraphs (b) and (c) to read as follows:

§ 64.6305 Robocall mitigation and certification.

* * * * *

(b) *Certification and database.* (1) Not later than the date established in a document released by the Wireline Competition Bureau establishing the Robocall Mitigation Database and portal (amending this paragraph (b)), a voice service provider, regardless of whether it is subject to an extension granted under § 64.6304, shall certify to one of the following:

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with § 64.6301(a)(1) and (2);

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it originates on that portion of its network are compliant with § 64.6301(a)(1) and (2), and the remainder of the calls that originate on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section; or

(iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network, and all of the calls that originate on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section.

(2) A voice service provider that certifies that some or all of the calls that originate on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section shall include the following information in its certification:

(i) Identification of the type of extension or extensions the voice service provider received under § 64.6304, if the voice service provider is not a foreign voice service provider;

(ii) The specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program; and

(iii) A statement of the voice service provider's commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

(3) All certifications made pursuant to paragraphs (b)(1) and (2) of this section shall:

(i) Be filed in the appropriate portal on the Commission's website; and

(ii) Be signed by an officer in conformity with 47 CFR 1.16.

(4) A voice service provider filing a certification shall submit the following information in the appropriate portal on the Commission's website.

(i) The voice service provider's business name(s) and primary address;

(ii) Other business names in use by the voice service provider;

(iii) All business names previously used by the voice service provider;

(iv) Whether the voice service provider is a foreign voice service provider; and

(v) The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues.

(5) A voice service provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (b)(2) through (4) of this section.

(c) *Intermediate provider and voice service provider obligations.* Beginning ninety days after the deadline for certifications filed pursuant to paragraph (b) of this section, intermediate providers and voice service providers shall only accept calls directly from a voice service provider, including a foreign voice service provider that uses North American Numbering Plan resources that pertain to the United States to send voice traffic to residential or business

subscribers in the United States, if that voice service provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (b) of this section.

10. Effective [**INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, add § 64.6306 to read as follows:

§ 64.6306 Exemption.

(a) *Exemption for IP networks.* A voice service provider may seek an exemption from the requirements of § 64.6301 by certifying on or before December 1, 2020, that, for those portions of its network served by technology that allows for the transmission of SIP calls, it:

(1) Has adopted the STIR/SHAKEN authentication framework for calls on the Internet Protocol networks of the voice service provider, by completing the network preparations necessary to deploy the STIR/SHAKEN protocols on its network including but not limited to participation in test beds and lab testing, or completion of commensurate network adjustments to enable the authentication and validation of calls on its network consistent with the STIR/SHAKEN framework;

(2) Has agreed voluntarily to participate with other voice service providers in the STIR/SHAKEN authentication framework, as demonstrated by completing formal registration (including payment) and testing with the STI Policy Administrator;

(3) Has begun to implement the STIR/SHAKEN authentication framework by completing the necessary network upgrades to at least one network element—e.g., a single switch or session border controller—to enable the authentication and verification of caller identification information consistent with the STIR/SHAKEN standards; and

(4) Will be capable of fully implementing the STIR/SHAKEN authentication framework not later than June 30, 2021, which it may only determine if it reasonably foresees that it will have completed all necessary network upgrades to its network infrastructure to enable the authentication and verification of caller identification information for all SIP calls exchanged with STIR/SHAKEN-enabled partners by June 30, 2021.

(b) *Exemption for non-IP networks.* A voice service provider may seek an exemption from the requirement to upgrade its network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework as required by § 64.6301 throughout its network by June 30, 2021, and from associated recordkeeping and reporting requirements, by certifying on or before December 1, 2020, that, for those portions of its network that do not allow for the transmission of SIP calls, it:

(1) Has taken reasonable measures to implement an effective call authentication framework by either:

(i) Upgrading its entire network to allow for the initiation, maintenance, and termination of SIP calls, and fully implementing the STIR/SHAKEN framework as required in § 64.6301 throughout its network; or

(ii) Maintaining and being ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-Internet Protocol caller identification authentication solution, or actively testing such a solution; and

(2) Will be capable of fully implementing an effective call authentication framework not later than June 30, 2021, because it reasonably foresees that it will have completed all necessary network upgrades to its network infrastructure to enable the authentication and verification of caller identification information for all non-Internet Protocol calls originating or terminating on its network as provided by a standardized caller identification authentication framework for non-Internet Protocol networks by June 30, 2021.

(c) *Certification submission procedures.* All certifications that a voice service provider is eligible for exemption shall be:

(1) Filed in the Commission's Electronic Comment Filing System (ECFS) in WC Docket No. 20-68, Exemption from Caller ID Authentication Requirements, no later than December 1,

2020;

(2) Signed by an officer in conformity with 47 CFR 1.16; and

(3) Accompanied by detailed support as to the assertions in the certification.

(d) *Determination timing.* The Wireline Competition Bureau shall determine whether to grant or deny timely requests for exemption on or before December 30, 2020.

(e) [Reserved]

11. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, adding paragraph (e) to read as follows:

§ 64.6306 Exemption.

* * * * *

(e) *Implementation verification.* All voice service providers granted an exemption under paragraphs (a) and (b) of this section shall file an additional certification consistent with the requirements of paragraph (c) of this section on or before a date specified in a document issued by the Wireline Competition Bureau (amending this paragraph (e)) that attests to whether the voice service provider fully implemented the STIR/SHAKEN authentication framework because it completed all necessary network upgrades to its network infrastructure to enable the authentication and verification of caller identification information for all SIP calls exchanged with STIR/SHAKEN-enabled partners by June 30, 2021. The Wireline Competition Bureau, after issuing a Public Notice seeking comment on the certifications, will, not later than four months after the deadline for filing of the certifications, issue a Public Notice identifying which voice service providers achieved complete implementation of the STIR/SHAKEN authentication framework.

(1) If a voice service provider cannot certify to full implementation upon the filing of this second certification, but demonstrates to the Wireline Competition Bureau that:

(i) It filed its initial certification in good faith—i.e., with a reasonable expectation that it would be able to achieve full implementation as initially certified; and

(ii) It made a good faith effort to complete implementation, the consequence for such a shortcoming is the loss of the exemption and the application of the implementation requirements of §§ 64.6301 and 64.6303, effective immediately upon release by the Wireline Competition Bureau of the Public Notice identifying which voice service providers achieved full implementation of the STIR/SHAKEN authentication framework.

(2) If a voice service provider cannot certify to full implementation upon the filing of this second certification, and the Wireline Competition Bureau finds that the voice service provider filed its initial certification in bad faith or failed to make a good faith effort to complete implementation, then:

(i) The voice service provider is required to fully implement the STIR/SHAKEN authentication framework immediately upon release by the Wireline Competition Bureau of the Public Notice identifying which voice service providers achieved full implementation of the STIR/SHAKEN authentication framework; and

(ii) The Wireline Competition Bureau shall refer the voice service provider to the Enforcement Bureau for possible enforcement action based on filing a false initial certification.

12. Effective [**INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, add § 64.6307 to read as follows:

§ 64.6307 Line item charges.

Providers of voice service are prohibited from adding any additional line item charges to consumer or small business customer subscribers for the effective call authentication technology required by §§ 64.6301 and 64.6303.

(a) For purposes of this section, "consumer subscribers" means residential mass-market subscribers.

(b) For purposes of this section, "small business customer subscribers" means subscribers that are business entities that meet the size standards established in 13 CFR part 121, subpart A.

[FR Doc. 2020-24904 Filed: 11/16/2020 8:45 am; Publication Date: 11/17/2020]